MASTER EN INGÉNIEUR DE GESTION À FINALITÉ SPÉCIALISÉE EN ANALYTICS & DIGITAL BUSINESS

L'évaluation globale des risques dans la lutte contre le blanchiment de capitaux et le financement du terrorisme

efficacité et enjeux

Lawarée, Aurélie

Award date:
2020

Awarding institution:
Universite de Namur

L’évaluation globale des risques dans la lutte contre le blanchiment de capitaux et le financement du terrorisme : efficacité et enjeux

Aurélie LAWARÉE

Directeur : Prof. L. GATOT

Mémoire présenté
en vue de l'obtention du titre de
Master 120 en Ingénieur de gestion,
à finalité spécialisée en Analytics & Digital Business

ANNEE ACADEMIQUE 2019-2020

Université de Namur, ASBL
Faculté des Sciences économiques, sociales et de gestion – Département des Sciences de gestion

Rempart de la Vierge 8, B-5000 Namur, Belgique, Tel. +32 [0]81 72 48 41/49 58, Fax +32 [0]81 72 48 40

AVANT-PROPOS

C'est avec grand plaisir que je dédie ces lignes en signe de gratitude et de reconnaissance à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail.

Je tiens tout d'abord à remercier mon directeur de mémoire, Laurent Gatot, pour ses précieux conseils, sa patience, sa disponibilité et surtout la confiance qu'il m'a accordée tout au long de la réalisation de ce mémoire.

Je remercie également l'établissement de crédit étudié et ses experts, pour leur collaboration et le partage de leur expérience de terrain dans la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Enfin, je remercie chaleureusement mes proches pour leur soutien indéfectible et leurs encouragements inestimables tout au long de mon parcours universitaire. Ils se reconnaîtront.

« *L'argent est moins important que*
la façon dont il a été gagné. »

(Hervé Desbois)

TABLE DES MATIERES

ABRÉVIATIONS & ACRONYMES

AES	Autorités Européennes de Surveillance
AML	Anti-Money Laundering
AMLCO	Anti-Money Laundering Compliance Officer
BC/FT	Blanchiment de Capitaux et Financement du Terrorisme
BNB	Banque Nationale de Belgique
BWRA	Business-Wide Risk Assessment
CBO	Chicago Board Option exchange
COE	Council Of Europe
CRF	Cellule de Renseignements Financiers
CTIF	Cellule de Traitement des Informations Financières
EI	Etat Islamique
FATF	Financial Action Task Force
FMI	Fond Monétaire International
GAFI	Groupe d'Action Financière
IA	Intelligence Artificielle
LBC/FT	Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme
OCAM	Organe de Coordination pour l'Analyse de la Menace
OCDE	Organisation de Coopération et de Développement Économiques
ONU	Organisation des Nations Unies
PPE	Personnes Politiquement Exposées
PSP	Prestataires de Services de Paiement
RBA	Risk Based Approach
REM	Rapport d'Évaluation Mutuelle
UBO	Ultimate Beneficial Owner
UE	Union Européenne
UNODC	United Nations Office on Drugs and Crime

INTRODUCTION

Initiative internationale mise en place il y a une trentaine d'année, la lutte contre le blanchiment de capitaux visait principalement, à cette époque, les nombreux trafiquants de drogue qui parvenaient à dissimuler l'origine illicite de leurs fonds en les réinvestissant dans l'économie légale.

L'intégration des mesures contre le financement du terrorisme n'est intervenue qu'une dizaine d'années plus tard, suite aux attentats du 11 septembre 2001 qui ont touché de plein fouet les États-Unis et secoué la planète entière.

À première vue, ces deux infractions, le blanchiment de capitaux et le financement du terrorisme, sont fondamentalement opposées. La première cherche à masquer l'origine illicite des fonds et l'autre cherche à masquer l'utilisation illicite des fonds. Le blanchiment poursuit un but économique tandis que celui du terrorisme et de son financement est essentiellement politique. Néanmoins, ce sont deux activités financières illégales à caractère transnational qui, finalement, requièrent des moyens de lutte assez similaires : une coopération internationale favorisant l'échange d'informations et une surveillance accrue des différents flux financiers pour permettre de détecter et geler au plus vite les fonds suspects.

Depuis lors, de nombreux facteurs ont favorisé l'expansion de ces deux criminalités à l'échelle mondiale. Parmi ceux-ci, nous retrouvons par exemple l'ouverture des frontières, la libre circulation des capitaux, le développement des transferts financiers électroniques, l'arrivée des crypto-actifs sans oublier les avancées en matière d'innovation technologique.

Qu'il s'agisse du blanchiment de capitaux ou du financement du terrorisme, ces deux phénomènes sont toujours au cœur de l'actualité et des préoccupations nationales. En effet, il n'est plus surprenant de voir la presse dénoncer de nouveaux scandales financiers, touchant généralement des dirigeants politiques, des hommes d'affaires influents, de grands groupes financiers et dévoilant parfois des montants assez spectaculaires. Bien qu'il soit hasardeux de chiffrer le blanchiment, sa nature l'excluant des statistiques économiques traditionnelles, le juge d'instruction spécialisé dans la criminalité financière, Michel Claise, estimait le montant de la fraude entre 4% à 6% du PIB belge, soit environ 24 milliards en 2017. En outre, la vague d'attentats ayant sévi en Europe ces dernières années n'a pas épargné la Belgique qui a, non seulement été ciblée plusieurs fois, mais a également abrité certaines cellules terroristes impliquées dans ces événements dramatiques. Il devient alors intéressant d'analyser les récentes mesures mises en place par la Belgique pour lutter contre ces deux phénomènes.

Ce mémoire n'a pas pour ambition d'honorer toutes les facettes de la lutte contre le blanchiment et le financement du terrorisme, ce qui s'avèrerait illusoire. L'objectif de cette étude est de comprendre

le fonctionnement du dispositif préventif de lutte contre le blanchiment de capitaux et le financement du terrorisme mis en place en Belgique pour ensuite analyser une partie des changements récemment apportés par la Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces.

Afin d'encadrer cette étude, la première partie définira les concepts de blanchiment de capitaux et financement du terrorisme. Ensuite, les moyens de lutte mis en place au niveau international et national seront exposés. Nous nous pencherons également de façon plus précise sur un des fondements essentiels du dispositif préventif actuel : l'approche fondée sur les risques.

Après avoir défini de façon précise la problématique étudiée et la méthode utilisée, la seconde partie de ce travail se concentrera sur la mise en œuvre du processus d'évaluation globale des risques, nouvelle obligation instaurée par la Loi du 18 septembre 2017. Elle analysera, dans un premier temps, le cas particulier d'un établissement de crédit puis, dans un second temps, les observations plus générales relatives aux institutions financières sous le contrôle de la Banque Nationale de Belgique. Enfin, cette étude développera également une partie des enjeux actuels de la lutte contre le blanchiment des capitaux et le financement du terrorisme en Belgique et apportera quelques pistes de solutions pour améliorer l'efficacité des dispositifs actuellement mis en place par les acteurs de cette lutte.

PREMIÈRE PARTIE : CADRE CONCEPTUEL

Chapitre 1 : Le blanchiment de capitaux

1.1. La définition du blanchiment de capitaux

Dater les origines du blanchiment de capitaux reviendrait à remonter à l'origine de la monnaie ou du moins, à l'époque trouble des « bonnes » ou « mauvaises » monnaies médiévales. L'utilisation de l'expression « blanchiment d'argent » coïncide avec la montée en puissance des grandes organisations criminelles aux États-Unis à l'époque de la prohibition[1] (VERNIER, 2017). Selon certains, elle ferait référence aux différentes blanchisseries ouvertes par certaines familles mafieuses pour dissimuler l'origine frauduleuse de leurs fonds. Ce type de commerce, générateur d'un nombre important d'espèces, permettait aux blanchisseurs d'ajouter les recettes de leurs activités illégales à celles du commerce donnant ainsi une existence légale à cet argent sale. Ce terme apparaît pour la première fois dans la littérature en 1973, à propos de l'affaire du Watergate[2], pour décrire la transformation des fonds actifs illicites en argent licite. (SCHNEIDER & WINDISCHBAUER, 2010, pp. 2-4)

Le concept juridique de blanchiment de capitaux émerge seulement dans les années 80, lorsque les acteurs économiques se rendent compte de la nécessité de lutter contre ce phénomène qui a pris une ampleur considérable grâce à la globalisation et à la dérégulation de l'économie. Il ne concerne plus seulement quelques familles mafieuses américaines mais bien des organisations criminelles de mieux en mieux organisées, dont les sources de revenus illégaux sont devenues polyvalentes (CHAPPEZ, 2003, p. 543). Les organisations internationales décident alors de mettre en place une stratégie commune de lutte contre le blanchiment de capitaux et de définir les infractions ainsi que les sanctions liées à celui-ci à travers différentes mesures législatives comme la Déclaration de Bâle du 12 décembre 1988 et la Convention des Nations unies contre le trafic illicite de stupéfiants et de substances psychotropes du 20 décembre 1988, signée à Vienne.

Ce travail se basera sur la définition proposée par la législation belge pour délimiter le concept de blanchiment de capitaux. La loi du 18 septembre 2017 relative à la prévention du blanchiment de

[1] Désigne une période de 1919 à 1933 durant laquelle une loi a tenté d'interdire l'importation, la fabrication et la vente d'alcool aux États-Unis ayant pour effet une forte augmentation de la criminalité et de la corruption.

[2] Affaire d'espionnage politique révélant des pratiques illégales au sein même de l'administration présidentielle des Etats-Unis aboutissant à la démission du président en fonction, Richard Nixon, en 1974.

capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces [ci-après nommée la « Loi »] définit le blanchiment de capitaux comme suit :

> *«*
>
> *- La conversion ou le transfert de capitaux ou d'autres biens, dont celui qui s'y livre sait qu'ils proviennent d'une activité criminelle ou d'une participation à une telle activité, dans le but de dissimuler ou de déguiser l'origine illicite de ces capitaux ou biens ou d'aider toute personne impliquée dans une telle activité à échapper aux conséquences juridiques des actes qu'elle a commis ;*
>
> *- Le fait de dissimuler ou de déguiser la nature, l'origine, l'emplacement, la disposition, le mouvement ou la propriété réels des capitaux ou des biens ou des droits qui y sont liés, dont celui qui s'y livre sait qu'ils proviennent d'une activité criminelle ou d'une participation à une telle activité ;*
>
> *- L'acquisition, la détention ou l'utilisation de capitaux ou de biens, dont celui qui s'y livre sait, au moment où il les réceptionne, qu'ils proviennent d'une activité criminelle ou d'une participation à une telle activité ;*
>
> *- La participation à l'un des actes visés aux 1°, 2° et 3°, le fait de s'associer pour le commettre, de tenter de le commettre, d'aider ou d'inciter quelqu'un à le commettre ou de le conseiller à cet effet, ou de faciliter l'exécution d'un tel acte. »*

Cette définition ne se limite pas aux capitaux mais intègre la notion « d'autres biens », transposant ainsi de façon fidèle l'article 3 de la quatrième Directive *AML*[3] (2015/849) qui définit ces biens comme « *les actifs de toute nature, corporels ou incorporels, meubles ou immeubles, tangibles ou intangibles, ainsi que les documents ou instruments juridiques, sous quelque forme que ce soit, y compris électronique ou numérique, attestant la propriété de ces actifs ou de droits y afférents* ». De manière générale, la législation belge anti-blanchiment est basée sur cette directive européenne, présentée dans la section 3.2.

Le caractère intentionnel du délit de blanchiment est mis en avant par la législation belge dans la mesure où les biens proviennent d'une activité criminelle « d'origine ». En effet, le blanchiment de capitaux est une infraction de conséquence, c'est-à-dire qu'il est lié à une ou plusieurs infractions sous-jacentes.

La liste des crimes et délits précédant l'infraction de blanchiment est longue et variée. Si on associe souvent au blanchiment le trafic illicite de stupéfiants, la vente d'armes ou encore le

[3] *AML* pour *Anti-Money Laundering*

proxénétisme, il faut également mentionner la criminalité organisée, le terrorisme, le financement du terrorisme et de la prolifération des armes de destruction massive, le trafic et la traite d'êtres humains ou encore le trafic de main d'œuvre clandestine (CTIF, 2018, p.52).

En outre, la mondialisation économique et financière a repoussé les frontières du blanchiment de capitaux en offrant une place prépondérante à la criminalité financière « en col blanc ». Cette expression désigne toutes les infractions économiques et d'affaires telles que les fraudes fiscales graves, les fraudes sociales, les infractions liées à l'état de faillite, les abus de biens sociaux ou de confiance, les détournements, les délits d'initié, la corruption ou encore toutes sortes d'escroqueries (CTIF, 2013, p.41).

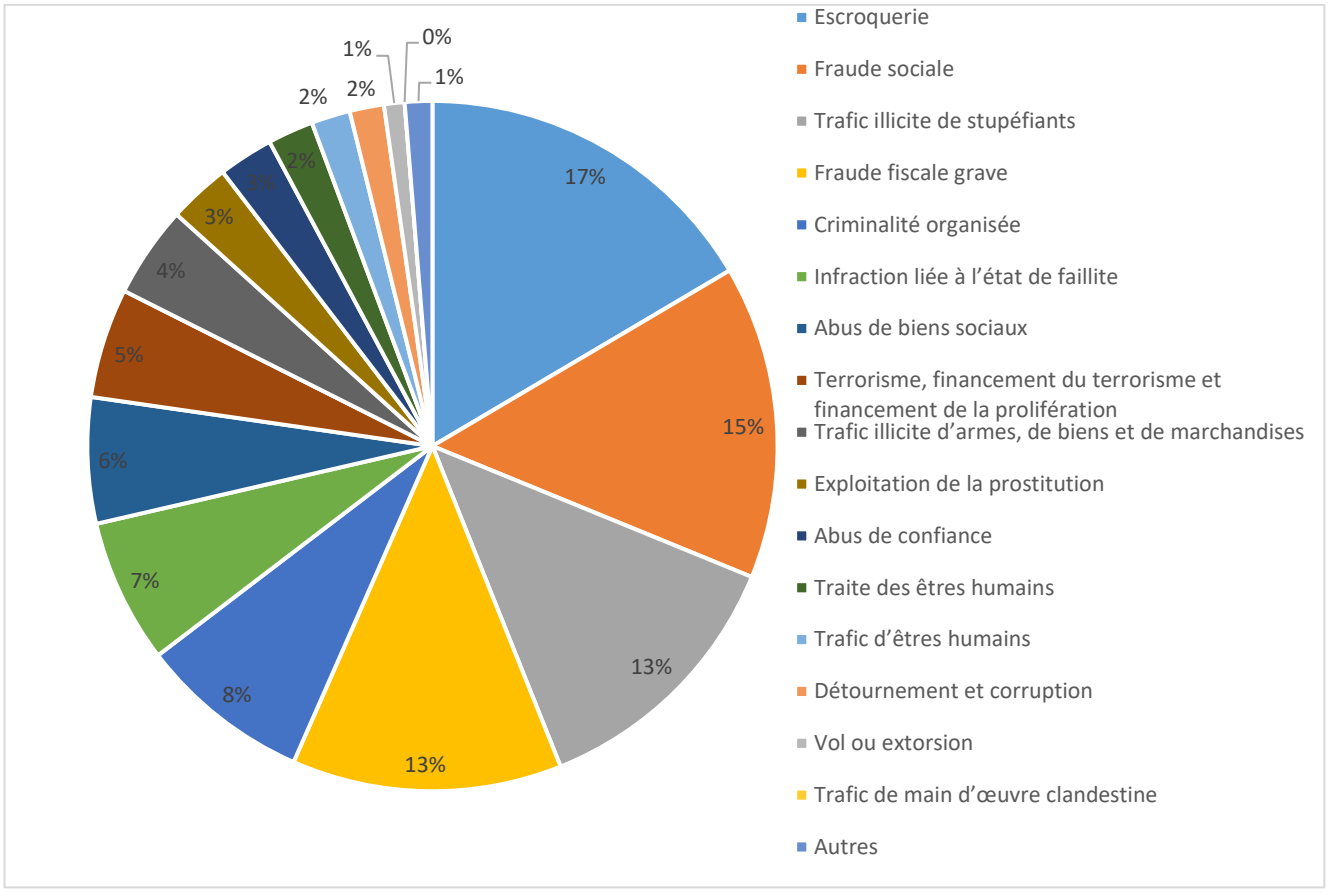
Pour lutter efficacement contre ces phénomènes, la Belgique a mis en place sa propre cellule de renseignement financier : la Cellule de Traitement des Informations Financières [ci-après CTIF]. Autorité administrative indépendante, son rôle principal est d'analyser les transactions financières suspectes portées à sa connaissance. Nous développerons plus en profondeur le fonctionnement de la CTIF à la section 4.2 de ce travail. Chaque année, cette Cellule publie un rapport annuel qui analyse, entre autres, les différents types d'infractions sous-jacentes présentes dans les 933 dossiers transmis au parquet en Belgique en 2018.

Il dévoile notamment le nombre de dossiers transmis par type de criminalités sous-jacentes principales. En observant la répartition de ces criminalités présentée au graphique 1.1, les quatre infractions les plus répandues en Belgique sont respectivement :

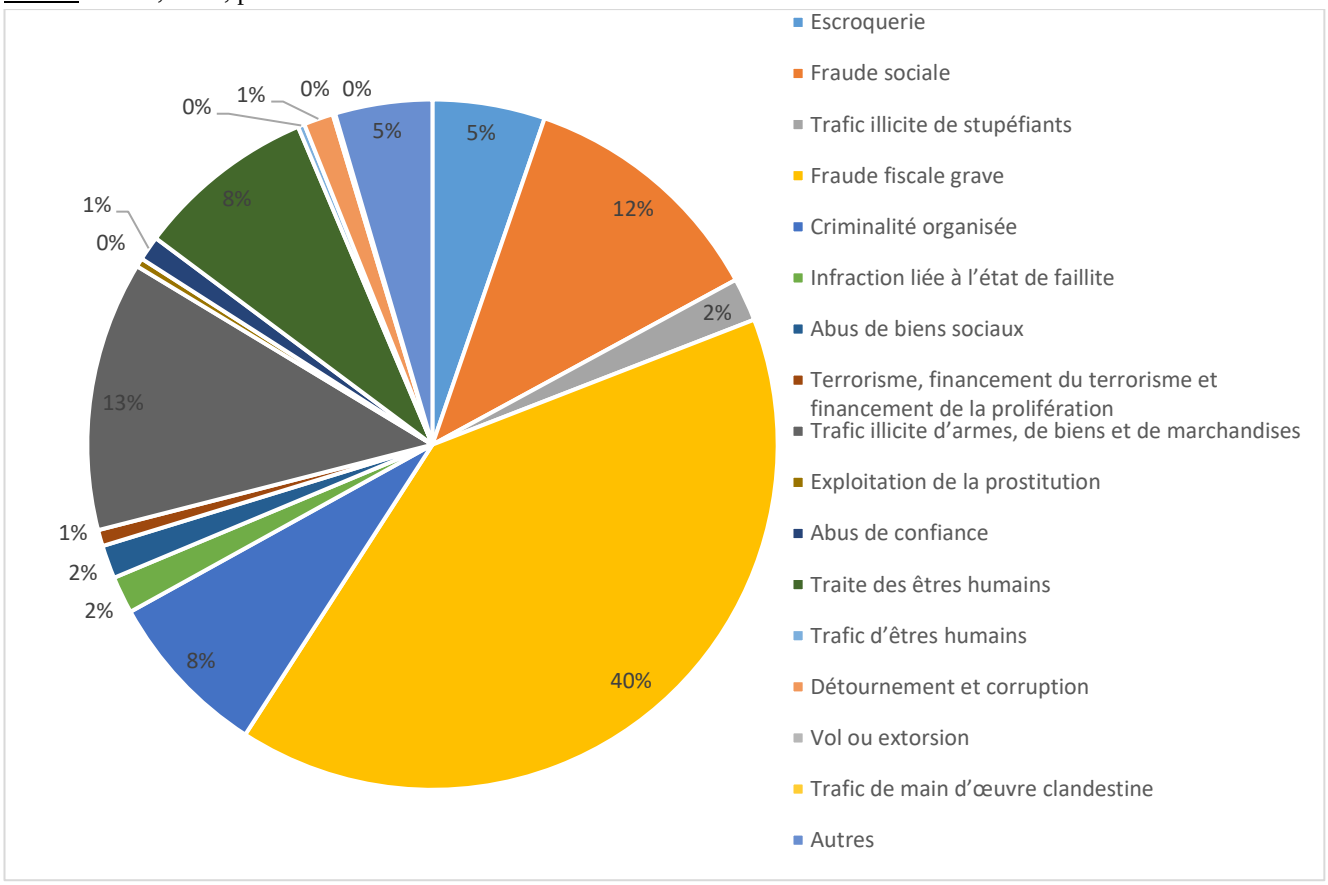
1) L'escroquerie
2) La fraude sociale
3) Le trafic illicite de stupéfiants
4) La fraude fiscale grave.

Toutefois, il est intéressant de se pencher également sur les montants relatifs à ces mêmes dossiers. En analysant leur répartition au graphique 1.2, les quatre infractions sous-jacentes les plus importantes obtenues cette fois sont respectivement :

1) La fraude fiscale grave
2) Le trafic illicite d'armes de biens et de marchandises
3) La fraude sociale
4) La traite des êtres humains.



Graphique 1.1 : Répartition du nombre de dossiers transmis par type de principale de criminalités sous-jacentes principales
Source : CTIF, 2018, p.52



Graphique 1.2 : Répartition des montants dans les dossiers transmis par type de criminalités sous-jacentes principales
Source : CTIF, 2018, p.55

La comparaison des deux graphiques (dont les couleurs correspondent aux mêmes infractions) nous indique que la répartition du nombre de dossiers transmis par type de criminalités sous-jacentes principales est différente de la répartition des montants traités dans ces mêmes dossiers. Ces données se complètent entre elles et mettent en évidence les infractions sous-jacentes les plus présentes en Belgique.

1.2. Le processus de blanchiment

Dans son premier rapport, le Groupe d'Action Financière [ci-après GAFI] a schématisé le processus des opérations de blanchiment en le divisant en trois phases distinctes : le placement, l'empilage et l'intégration.

Le placement, connu également sous le nom de « prélavage », d'« injection » ou d'« immersion », est la première phase du processus blanchiment. Elle consiste à introduire les fonds provenant directement d'une activité criminelle, souvent d'importantes sommes en liquide, dans le système financier. Les blanchisseurs fractionnent leurs bénéfices en de plus petites quantités d'espèces, moins suspectes, pour les déposer sur différents comptes bancaires. Ils peuvent également investir dans d'autres instruments monétaires comme des chèques, des devises étrangères, des ordres de virement ou d'autres biens comme l'or ou les diamants. (FATF-GAFI, 2019a) Cette étape, qui représente la jonction entre le système financier légal et les capitaux d'origine criminelle, est la plus délicate pour les blanchisseurs et la plus facilement détectable par les enquêteurs (UNODC, 2018).

Vient ensuite la phase d'empilage, appelée aussi « empilement », « dispersion » ou « lavage », qui consiste généralement en une succession de transactions entre plusieurs pays visant à séparer les capitaux de leur origine illégale et éviter ainsi leur traçabilité. Cette étape est souvent la plus sophistiquée parce que les méthodes utilisées par les blanchisseurs sont nombreuses et de plus en plus complexes. Les fonds peuvent être investis dans divers instruments de placement, utilisés pour payer des biens ou des services ou encore être dispersés sur différents comptes bancaires généralement situés dans des pays où ils pourront jouer sur les différences de règlementations entre les États, certains étant plus laxistes en matière de secret bancaire. (FATF-GAFI, 2019a)

La troisième phase, l'intégration ou encore « le recyclage », permet de rapatrier les capitaux désormais camouflés en argent d'apparence légale dans des activités économiques légitimes. A ce stade, les criminels ont l'opportunité d'utiliser les produits du crime à leur avantage en réinvestissant l'argent (FATF-GAFI, 2019a). Ces investissements poursuivent généralement trois objectifs :

- L'enrichissement personnel : l'acquisition de biens à usage personnel est le but même des activités criminelles. Les criminels utilisent ces fonds pour améliorer leur qualité de vie en achetant différents produits de luxe, résidences, yachts, avions, etc. ;
- Le développement des activités criminelles : suivant une logique d'investissement, les criminels réinjectent une partie des fonds blanchis dans le développement de leur « gagne-pain » et en particulier dans le système de blanchiment qu'ils ont mis en place. Ils vont ainsi acquérir de nouvelles « machines à laver », c'est-à-dire de nouvelles activités commerciales légitimes qui leur donnent la possibilité de dissimuler plus de fonds provenant d'activités criminelles, augmentant de façon continue leurs bénéfices.
- L'achat de la respectabilité : soucieux de blanchir non plus les fonds mais bien leur réputation, les criminels décident d'investir dans des activités complètement licites comme des opérations financières classiques, des investissements immobiliers ou la participation dans des entreprises. La présence d'associés respectables, issus de l'économie formelle, dans les montages financiers permet aux blanchisseurs de passer outre les procédures ou les contrôles classiques.
  (KOUTOUNIS et THONY, 2005, pp. 31-33)

Même s'il existe de nouvelles propositions d'approches moins théoriques et que la réalité est bien plus complexe aujourd'hui, cette classification facilite la compréhension du phénomène du blanchiment de capitaux.

1.3. L'impact sur l'économie

Chiffrer l'ampleur du blanchiment est un exercice assez hasardeux compte tenu de la nature occulte des infractions qui s'y rapportent. Les revenus générés par ces activités criminelles ne peuvent être comptabilisés comme de simples recettes commerciales dans les statistiques. Néanmoins, le Fond Monétaire International (FMI) estime que le montant des fonds blanchis ou destinés au financement du terrorisme représenterait entre 2.5 et 5% du PIB mondial, soit entre 400 et mille milliards d'euros (SPF ECONOMIE, 2019).

Si les coûts sociaux et humains de certaines infractions sous-jacentes comme la traite et le trafic d'êtres humains, le trafic illicite de stupéfiants, le financement du terrorisme ou encore l'exploitation de la prostitution sont assez évidents à mettre en lumière, l'impact économique du blanchiment d'argent et notamment de la criminalité en col blanc est parfois plus complexe à déterminer mais tout aussi conséquent.

Au niveau microéconomique, les secteurs où les blanchisseurs ont décidé d'investir pour créer leurs activités commerciales de façade risquent de subir une forme de concurrence déloyale. Les capitaux

réguliers se retrouvent mélangés aux produits d'activités illicites, entrainant ainsi une détermination des prix faussée dans certains secteurs tels que l'hôtellerie ou la restauration. Les prix concurrentiels pratiqués par ces commerces peuvent parfois aller jusqu'à empêcher d'autres entreprises du même secteur de s'implanter dans la même région. Ce contournement du principe d'égalité entre les acteurs expose l'économie à un risque de contamination, incitant les commerçants honnêtes à enfreindre la loi à leur tour pour faire perdurer leur affaire. (PEREIRA, 2011, p. 45)

A l'échelon macroéconomique, le FMI explique que la stabilité tout entière du secteur économique est potentiellement impactée par le blanchiment. Des variations inexplicables de la demande de monnaie et l'altération des indicateurs mettent en péril les politiques des grandes institutions monétaires. Les effets de contamination sur des opérations financières légales sont également présents et considérables à cette échelle. La stabilité des cours de change est quant à elle fragilisée suite au renforcement de l'instabilité des mouvements internationaux des capitaux et aux transferts transnationaux d'actifs inattendus. Ces mouvements difficiles à anticiper créent alors des problématiques de liquidité pour les banques. (FATF-GAFI, 2019a)

Un autre risque important pour les institutions financières est le risque d'atteinte à la réputation qui remet en question l'intégrité des marchés financiers, pilier fondamental pour le fonctionnement de ceux-ci. Si placer des fonds illicites provenant d'activités criminelles dans une institution financière devient une opération aisée, celle-ci pourrait être impliquée dans une complicité active avec des criminels au risque de devenir une composante du réseau criminel lui-même. Ce type d'accusations provoquerait inévitablement un manque de confiance dans l'institution de la part des clients mais aussi des autres intermédiaires financiers, déclenchant des retraits en masse. (PEREIRA, 2011, p. 45) Pour éviter de devoir faire face à ce genre de situation, certaines institutions financières n'hésitent pas à rompre purement et simplement leurs relations avec certains secteurs réputés « plus sensibles » tels que les diamantaires ou le monde du football. Dès lors, des secteurs entiers se retrouvent vers ces Cette pratique, qu'on appelle le *de-risking*, est interdite par les autorités de contrôle (Cf. Section 8.2).

Les effets du blanchiment de capitaux sont dévastateurs tant sur les économies développées que celles en développement.

Dans les pays développés, c'est la criminalité à col blanc qui met à mal les mécanismes de régulation et de redistribution des richesses, notamment au travers de la fraude fiscale. Les dirigeants politiques ou les hommes d'affaires qui mettent en place des mécanismes pour éviter certains impôts contribuent en fait aux difficultés financières de leur pays. Cette diminution des recettes fiscales de l'Etat engendre souvent la nécessité d'augmenter le taux d'imposition. Les fraudeurs ne font alors que déplacer

la charge de l'impôt sur les autres citoyens, ceux qui généralement ont moins de moyens mais le paient pleinement. Alors que les scandales de fraude dans le monde politique ne cessent d'être dévoilés et que les multinationales bénéficient de traitements de faveur, ce sont ces mêmes citoyens qui ne tolèrent plus les hausses de l'impôt et réclament plus de transparence. La « crise des gilets jaunes » en France peut être considérée comme un exemple de ce phénomène, où même la classe moyenne refuse ce partage fiscal qui leur paraît désormais inégalitaire. Dès lors, c'est la sécurité et la stabilité politique de ces pays développés qui sont directement impactées. (VERNIER, 2018)

Les économies dotées de centres financiers en expansion ou en cours de développement n'ont, en général, pas encore de politique ou de mesure de lutte contre le blanchiment de capitaux mise en place. Elles deviennent par conséquent des cibles très convoitées par les organisations criminelles qui cherchent à détourner les contraintes des autorités en profitant des disparités existantes entre les différents régimes nationaux. Le réseau et les capitaux sont alors déplacés vers ces centres financiers extraterritoriaux, plus cléments sur l'origine des capitaux. A court terme, ces différents pays ne peuvent se permettre d'être trop regardants quant aux investissements qu'ils attirent. Cependant, si les autorités ne régulent pas la situation assez rapidement, le risque à long terme est d'avoir une criminalité organisée enracinée et imbriquée dans le système politique grâce à la corruption des agents publics et des gouvernements. (FATF-GAFI, 2019a ; PEREIRA, 2011, p. 45)

Le blanchiment d'argent représente également un *manque à gagner* incalculable pour l'économie mondiale.

Prenons d'abord en compte les pertes monétaires directes dues aux différentes infractions sous-jacentes du blanchiment. En Belgique, le montant total dans les dossiers de blanchiment transmis au parquet s'élève à 1 432,73 millions d'euros uniquement pour l'année 2018 (CTIF, 2018, p.55).

A cela, il faut ajouter les montants consacrés à la lutte contre le blanchiment investis par les institutions, les entreprises ainsi que les contribuables depuis une trentaine d'années. Les différentes conventions, directives, lois, mesures mises en place au fil du temps demandent à chaque étape de nouveaux moyens tant humains que financiers qui auraient pu être investis dans d'autres causes. En 2018, 42% des entreprises participant à une enquête mondiale disaient avoir augmenté leurs dépenses pour lutter contre la fraude et la criminalité économique au cours des deux dernières années (PWC, 2018, p.6).

Néanmoins, il est important de rappeler que le blanchiment, infraction de conséquence, permet également aux activités criminelles qui le précèdent de perdurer. Un grand nombre d'investigations relatives à la lutte contre le blanchiment de capitaux aident à retrouver des fonds volés, à restituer l'argent aux victimes et affaiblissent également les réseaux criminels en les privant de financements utilisables.

Dès lors, la lutte contre le blanchiment de capitaux ne représente plus uniquement une « chasse à l'argent sale », mais elle est devenue un premier moteur d'investigation pour réduire la criminalité à travers le monde.

Pierre Kopp (2006, p.41) écrit : « *le décideur public doit arrêter de consacrer de l'argent à la répression du blanchiment lorsque le coût marginal de la répression devient supérieur à la réduction du coût social du blanchiment qu'elle permet d'atteindre* ». Les multiples retombées négatives citées ci-dessus nous laissent dès lors penser que la lutte anti-blanchiment a malheureusement encore de longs jours devant elle.

1.4. Les tendances en matière de blanchiment en Belgique

Dans son rapport annuel de 2018, la CTIF dévoile les dernières évolutions en termes de menaces criminelles auxquelles notre pays fait face actuellement. Cette analyse met en lumière les différentes infractions sous-jacentes qui prennent de l'ampleur, entrainent une hausse du blanchiment de capitaux en Belgique et méritent donc une attention particulière.

1.4.1. Le trafic de stupéfiants

La Belgique n'est pas seulement un pays de destination pour la drogue, elle est également un pays de transit et de production pour la plupart des substances illicites. L'importance de cette menace criminelle se reflète à travers une augmentation de 57%[4] du nombre de dossiers relatifs au trafic de stupéfiants transmis à la CTIF entre 2016 et 2018. Quant aux montants relatifs à ces dossiers, ils ont plus que doublé[5] en deux ans. Une partie des dossiers implique le recours à des commerces de couvertures actifs dans les secteurs générateurs de cash tels que l'HORECA ou les *night shops* dans lesquels les espèces issues du trafic sont mélangées aux recettes de l'activité commerciale. Des schémas de compensation[6] avec le secteur de la construction apparaissent également dans ces dossiers où les fonds illicites permettent de payer les travailleurs en « noir ». Le secteur du commerce de véhicules d'occasion

[4] 76 dossiers dont la criminalité sous-jacente principale est le trafic illicite de stupéfiants ont été transmis en 2016 contre 119 en 2018 (CTIF, 2018, p.52).

[5] Le montant relatif aux dossiers transmis dont la criminalité sous-jacente principale est le trafic illicite de stupéfiants s'élève à 14.22 millions d'euros en 2016 contre 29.03 millions en 2018 (CTIF, 2018, p.55).

[6] Les trafiquants s'associent avec des fraudeurs, ayant besoin d'utiliser des espèces pour alimenter leurs activités illégales, et leur remettent les liquidités en échange de transferts internationaux justifiés par de fausses factures.

est une aubaine pour les blanchisseurs qui utilisent des pratiques de *Trade based money laundering*[7] : les véhicules sont achetés en Europe, acheminés vers l'Afrique de l'Ouest et revendus au profit des trafiquants de stupéfiants. (CTIF, 2018, pp.11-12)

1.4.2. La traite des êtres humains

Cette infraction est devenue une des activités illicites les plus lucratives au sein de l'UE. Les réseaux de trafic et la traite d'êtres humains sont mobiles, transnationaux et possèdent une cellule dans les pays d'origine des victimes – principalement la Roumanie, la Hongrie, la Pologne, la Bulgarie, le Nigeria, l'Albanie, le Vietnam, la Chine et l'Érythrée – ainsi que dans leurs pays de transit et de destination. Internet et les réseaux sociaux participent au recrutement des victimes et soutiennent les plateformes commerciales de prostitution. Les flux financiers en rapport avec l'exploitation sexuelle sont généralement des transferts de types *money remittance*[8] à destination de pays réputés sensibles en matière de traite des êtres humains. Dans l'UE, la demande de main d'œuvre bon marché ne cesse de croitre, impactant ainsi l'exploitation par le travail. Plusieurs constructions frauduleuses comme des cascades de sous-traitants, de faux indépendants, de faux détachements de travailleurs de sociétés en Europe de l'Est sont mises en lumière dans les dossiers de la CTIF illustrant des pratiques de dumping social. Les liens avec la criminalité organisée sont de plus en plus fréquents mais ces pratiques de trafic et traite d'êtres humains sont plus présentes aux niveaux les plus bas des organisations, ce qui donne aux CRF une base d'enquête avant de remonter plus dans la hiérarchie. (CTIF, 2018, pp.13-14)

1.4.3. La corruption

Même si le nombre de dossiers transmis à la CTIF est relativement limité, les montants impliqués sont importants puisqu'on compte en moyenne 2,5 millions d'euros par dossier. La CTIF révèle qu'une grande partie des intervenants dans ces dossiers sont de nationalité belge et ne sont pas forcément des personnes politiquement exposées [ci-après PPE]. Il s'agit le plus souvent d'opérations financières « one shot », où un compte est ouvert uniquement pour effectuer des opérations de blanchiment. Une partie des dossiers concernent des transferts suspects liés à l'achat de biens immobiliers ou de luxe tandis que d'autres dossiers ont tendance à dissimuler le bénéficiaire effectif soit au travers d'intermédiaires financiers soit en impliquant des structures sociétaires opaques[9] situées dans des territoires à faible

[7] Pratiques où les profits illicites sont investis dans des produits ou services qui sont ensuite délocalisés ; c'est cette délocalisation qui leur donne une forme de légitimité et confère aux fonds une apparence légale.

[8] Désigne les transferts d'argent réalisés par un travailleur étranger vers une personne dans son pays d'origine.

[9] Il s'agit fréquemment de *Limited*, de fondations, de *trusts* ou des *Free Zone Establishments*.

fiscalité. De fausses factures de prestations aux communications vagues apportent une justification économique à ces transferts de fonds. (CTIF, 2018, pp.14-16)

1.4.4. L'escroquerie

Aujourd'hui, l'escroquerie se manifeste à travers des réseaux organisés, spécialisés, internationaux et dynamiques qui varient constamment leurs techniques pour saisir chaque nouvelle opportunité. Parmi les méthodes de fraudes récemment utilisées, la CTIF cite plusieurs variantes telles que les escroqueries aux virements frauduleux, les fraudes au président[10] ou encore les escroqueries liées à des sites de trading non régulés, à des placements en diamants d'investissement ou à des plateformes de trading en crypto-monnaies. Les opérations de blanchiment liées à ces escroqueries sont souvent opérées par des réseaux de blanchisseurs professionnels et suivent généralement les circuits habituels : mise en place de schémas de compensation, transferts de fonds vers l'étranger, comptes de transit ouverts au nom de sociétés écrans, fausses factures, … (CTIF, 2018, pp.16-17)

[10] Escroquerie souvent liée à la corruption des e-mails professionnels, elle consiste à se faire passer pour le dirigeant d'une société afin d'obtenir le paiement d'une somme d'argent de la part d'un employé par le biais d'un virement. (DEMPURÉ, 2017)

Chapitre 2 : Le financement du terrorisme

2.1. La définition du financement du terrorisme

Avant de parler de son financement ou de ses origines, il est important de définir le terme "terrorisme" au vu de ses nombreuses connotations politiques, morales et religieuses. En 1999, les Nations Unies l'ont défini dans la Convention internationale pour la répression du financement du terrorisme, convention reprise par la 35ème recommandation du GAFI (Cf. Annexe 1, Les recommandations du GAFI). L'article 2 de cette convention définit le terrorisme comme suit :

«

- *Un acte qui constitue une infraction au regard et selon la définition de l'un des traités énumérés en annexe (de la Convention) ;*
- *Tout autre acte destiné à tuer ou blesser grièvement un civil, ou toute autre personne qui ne participe pas directement aux hostilités dans une situation de conflit armé, lorsque, par sa nature ou son contexte, cet acte vise à intimider une population ou à contraindre un gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque. »*

Comme le dit l'expression populaire, l'argent est le nerf de la guerre. Le terrorisme a un besoin de ressources évident pour pouvoir mener à bien ses idéologies et financer les dépenses de l'organisation. En Belgique, le 3ème article de la Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces définit le financement du terrorisme comme suit :

> « *le fait de réunir ou de fournir des fonds ou d'autres moyens matériels, par quelque moyen que ce soit, directement ou indirectement, avec l'intention qu'ils soient utilisés ou en sachant qu'ils seront utilisés, en tout ou en partie, par une organisation terroriste ou par un terroriste agissant seul, même en l'absence de lien avec un acte terroriste précis*. »

Cette définition ne vise donc pas uniquement les actes terroristes précis comme les attentats, mais également le financement général d'une organisation terroriste, qui assure ainsi la survie mais surtout l'expansion de ces groupes.

Notons que même si le financement du terrorisme est repris dans la liste des infractions sous-jacentes au blanchiment de capitaux, ces deux concepts diffèrent sur l'objectif et la motivation des parties.

Contrairement au blanchiment de capitaux, l'objectif premier du financement du terrorisme n'est pas de masquer l'origine illégale des capitaux mais plutôt de rompre le lien entre les capitaux et leur destination où ceux-ci seront utilisés à des fins terroristes. Comme le souligne HANE (2015, p.48) « *Par rapport au crime, le blanchiment est une conséquence tandis que le financement du terrorisme est un moyen ou une condition* ».

Cette différence se marque également dans la divergence de motivation entre criminalités organisées et organisations terroristes. Les premières ont comme finalité essentielle le profit alors que pour les secondes, l'argent est un outil au service d'une cause. L'économie terroriste oriente continuellement l'utilisation de ses fonds autour de l'accomplissement d'un objectif idéologique ou politique (KOUTOUZIS ET THONY, 2005, p.21).

Nous en venons à nous demander pourquoi la lutte contre le blanchiment de capitaux et celle contre le financement du terrorisme sont assimilées dans de nombreuses législations.

Premièrement, la finalité de ces deux politiques de lutte est la même : affaiblir le pouvoir économique criminel – ou terroriste – accumulé par certaines organisations. Lorsque leur ampleur est devenue trop importante, les institutions de l'Etat ne pouvaient plus gagner en les attaquant de front et ont alors décidé de frapper un point sensible, c'est-à-dire leurs sources de revenus et leur capacité à lever des fonds (KOUTOUZIS ET THONY, 2005, p.22).

Deuxièmement, le blanchiment de capitaux et le financement du terrorisme sont deux activités financières illégales à caractère transnational. Dès lors, ces deux infractions requièrent les moyens de lutte semblables : une coopération internationale pour favoriser l'échange d'informations ainsi qu'une surveillance accrue des différents flux financiers pour détecter et geler au plus vite les fonds suspects (CTIF, 2015a, p.25). C'est dans cette logique qu'en 2001, après les attentats du 11 septembre, le GAFI a étendu son mandat pour mettre les différentes compétences déjà acquises au cours de la lutte anti-blanchiment au service de la lutte contre le financement du terrorisme en s'attaquant à ses sources de financement.

2.2. Les principales sources du financement du terrorisme

Les sources du financement du terrorisme sont relativement variées. Nous les regrouperons en trois grandes catégories : le financement par les États, le macro-financement et le micro-financement.

2.2.1. Le financement par les États

La participation des États aux activités terroristes a évolué au cours du temps mais reste une problématique actuelle. Un pas en arrière dans l'histoire nous permet d'expliquer cette évolution.

Depuis la seconde guerre mondiale jusqu'à la fin de la guerre froide, le financement par les États représentait la source de revenus principale des organisations terroristes. Que ce soit en Amérique centrale, en Irlande, en Iran, en Afghanistan ou encore en Europe, différentes motivations politiques et économiques ont entrainé les grandes puissances à soutenir et financer différents groupements terroristes; pour finalement en être les victimes aujourd'hui, comme l'explique à travers une multitude d'exemples l'ouvrage de KOUTOUZIS ET THONY (2005). Dès 1995, l'ONU adopte diverses mesures visant à éliminer le terrorisme international. La résolution 49/60 recondamne fermement le terrorisme, rappelle aux États les obligations imposées par la Charte des Nations Unies et les prie également :

> *«*
>
> *[…] De s'abstenir d'organiser, de fomenter, de faciliter, de financer, d'encourager ou de tolérer des activités terroristes et de prendre les mesures pratiques voulues pour que leur territoire ne serve pas à des installations ou à des camps d'entraînement de terroristes, ni à la préparation ou à l'organisation d'actes terroristes à l'encontre d'autres États ou de leurs ressortissants; […] »*

Par la suite, à l'aide des nouvelles mesures de lutte anti-terrorisme mises en place et constamment actualisées, la participation directe des États au financement du terrorisme a nettement diminué.

Il reste cependant un risque pour ces derniers de participer de façon indirecte au maintien des organisations terroristes. Certains groupes ont pris le contrôle de ressources économiques comme le pétrole (voir infra p.19) et les réinsèrent sur le marché mondial en dissimulant (ou non) leur provenance. Le risque pour les États de traiter avec les intermédiaires financiers au service de ces groupes devient alors important et il est de leur responsabilité de se renseigner correctement sur ces échanges. Nous faisons référence à un problème d'actualité puisqu'en 2015, le Conseil de sécurité a pris en compte cette forme de financement du terrorisme dans la résolution 2199 en condamnant fermement :

> «
>
> *[…] toute participation au commerce direct ou indirect, en particulier de pétrole et de produits pétroliers, d'unités de raffinage modulaires et de matériels connexes avec l'EIIL, le Front el-Nosra et tous autres personnes, groupes, entreprises et entités désignés comme étant associés à Al-Qaida par le Comité (…) et réaffirme que cette participation équivaudrait à soutenir financièrement ces personnes, groupes, entreprises et entités et pourrait conduire le Comité à inscrire de nouveaux noms sur sa Liste relative aux sanctions;[…]* »

Même si les États jouent aujourd'hui un rôle moindre dans le financement du terrorisme, ils se doivent de rester vigilants face à la présence des organisations terroristes au cœur de l'économie de marché.

2.2.2. Le macro-financement

Lorsque le soutien financier des États a diminué, les organisations terroristes ayant survécu ont trouvé d'autres moyens de ressources et se sont tournées vers les activités criminelles comme le trafic d'armes, le trafic d'êtres humains, l'escroquerie, la contrefaçon, le trafic de biens et de marchandises mais surtout le trafic des stupéfiants (CTIF, 2015b, p.10). Le terrorisme, imbriqué ainsi de manière ponctuelle dans les réseaux criminels souterrains, a un impact significatif sur le développement et la prolifération de la criminalité organisée.

Parmi les sources illégales de financement du terrorisme, on trouve également la *ghanima*, le butin de guerre, c'est-à-dire le financement par actes délictueux (BOUTRY & DÉCUGIS, 2018). Comme l'explique BENRAAD (2015), les organisations terroristes ont l'habitude de s'accaparer les infrastructures et les ressources des territoires sous leur domination. L'exploitation de ces produits de guerre est variée :

1) Les sites archéologiques et les propriétés luxueuses sont pillés pour revendre les vestiges et antiquités sur le marché noir.
2) Les maisons, les commerces et les restaurants sont victimes d'extorsions ou d'expropriations justifiées au nom de la « protection » soi-disant assurée par l'organisation terroriste. Celles-ci vont parfois jusqu'à réclamer des impôts aux populations ou encore des taxes sur certains biens, recréant ainsi un véritable système fiscal.
3) Les banques, publiques et privées, sont mises à sac pour ensuite être contrôlées par l'organisation et faciliter ainsi le détournement des devises locales, le pillage des succursales, les ponctions imposées sur les transferts d'argent tout en favorisant les transferts de capitaux d'origine illicite.
4) Les ressources naturelles, hydrauliques et énergétiques des territoires conquis sont exploitées au profit de l'organisation puis revendues à des prix concurrentiels sur les marchés régionaux via des intermédiaires financiers autonomes présents sur les marchés internationaux. Par exemple, l'Etat Islamique [ci-après EI] aurait vendu pour 850 000 dollars de pétrole par jour en 2014.
5) L'agriculture locale, protégée par la coalition internationale qui ne peut pas bombarder ce genre d'exploitations, est elle aussi placée sous le contrôle de l'organisation. Ces exploitations agricoles représentent une source de revenus importants et réguliers comme l'explique Frédéric JOUVET (2018) dans le quotidien L'écho, selon lequel la vente d'orge pouvait rapporter 1.9 million de dollars à l'EI en une seule journée.

Le tableau décrit ci-dessus démontre bien l'évolution de l'économie de guerre vers un système de gouvernance et atteste d'une véritable forme d'ingénierie financière et d'autofinancement de la part des organisations terroristes.

Aujourd'hui, les facilités du système financier international représentent également une possibilité de financement pour les organisations terroristes en leur offrant une multitude d'instruments financiers accessibles sous le couvert de l'anonymat. Une connaissance des marchés ou quelques intermédiaires corrompus situés aux bons endroits leur donne la possibilité de faire fructifier rapidement l'argent destiné au financement du terrorisme.

L'exemple le plus parlant est l'analyse des contrats d'option de vente[11], effectués entre le 6 et le 10 septembre 2001, sur les compagnies aériennes utilisées lors des attentats – American Airlines, United Airlines – ou aux sociétés qui avaient des bureaux dans les tours du World Trade Center – Morgan Stanley, Merrill Lynch, Citigroup (TREFFEL, 2015). Si l'on prend le cas d'American Airlines, 1 535 contrats d'options de ventes à échéance octobre 2001 ont été traités au CBOE[12] le 10 septembre, contre une moyenne quotidienne de 24 contrats dans les trois semaines précédentes. Les scénarios sont similaires pour les autres sociétés citées supra, générant ainsi plusieurs dizaines de millions de dollars de bénéfices pour les détenteurs de ces options (ALCARAZ, 2007).

Même si l'enquête a été fermée sans conclure sur des résultats probants, ces volumes atypiques resteront aussi troublants que l'idée même que les terroristes puissent spéculer sur les effets économiques de leurs massacres …

2.2.3. Le micro-financement

Même si la 'petite délinquance' apparaît comme une ressource pour le financement du terrorisme, il est important de souligner que les fonds affectés à cette cause peuvent avoir une origine tout à fait légale (CTIF, 2016, p.30).

Les organisations terroristes s'appuient sur des fonds provenant de la charité, la *zakat* (BOUTRY et DÉCUGIS, 2018). Ce type de financement repose principalement sur des dons effectués sous le couvert d'organisations caritatives qui militent par exemple pour améliorer les conditions de vie des réfugiés ou des orphelins de guerre. Les profils des donateurs – volontaires ou non – peuvent varier : riches sponsors établis dans des pays du Golfe comme l'Arabie Saoudite ou le Qatar, entreprises privées ou simples citoyens désireux de participer à une bonne cause. Ces associations humanitaires confèrent aux fonds récoltés la façade d'une cause légale et légitime en évitant donc tout soupçon ou enquête pour financement du terrorisme (BENRAAD, 2015, p.8).

[11] Contrat permettant à son acquéreur de vente un actif sous-jacent à un prix et une date déterminés à l'avance

[12] *Chicago Board Option Exchange* : bourse renommée située aux Etats-Unis où se négocie principalement des contrats d'option

Eviter le système bancaire permet aux organisations terroristes de ne pas attirer l'attention des autorités et de protéger tant la source des fonds que leur destinataire. C'est pourquoi elles ont recours encore aujourd'hui à certains systèmes parallèles de transferts de fonds informels, les *hawalas* (SPF ECONOMIE, 2019). Les *hawalas* sont utilisés pour pallier les défaillances des institutions financières dans les pays où la situation politique est précaire ou fragile. Le but de ce système est d'offrir aux populations locales des services de transferts d'argent pour que les membres de familles vivant dans des pays riches puissent soutenir financièrement ceux restés dans ces pays où l'instabilité règne. Le principe de base est de faire circuler l'argent d'un pays A vers un pays B via un réseau d'agences d'*hawalas* qui prennent de petits pourcentages, une compensation, sur chaque transaction (Cf. Annexe 2, Le fonctionnement de l'*hawala*). Aucune règle formelle ne régissant ces transactions, une telle opacité finit par attirer non seulement les réseaux mafieux voulant faire circuler les bénéfices de leurs activités criminelles mais également les partisans des organisations terroristes qui souhaitent financer leur idéologie (MAHAMOUD, 2014).

2.3. Les besoins financiers du terrorisme

Même si les différentes organisations terroristes varient en fonction de leur taille, de leur structure, de leurs motivations, elles ont toutes en commun un besoin de financement. Pour comprendre les différents besoins financiers des acteurs du terrorisme, il faut distinguer le financement de l'organisation terroriste en elle-même et le financement des actes terroristes isolés ou des petites cellules (CTIF, 2015b, p.23).

Les coûts opérationnels des structures terroristes de grande ampleur, comme l'Etat Islamique ou Al-Qaïda, sont considérables et requièrent d'importantes sources de financement – ce que l'on appelle le macro-financement. Ils sont répartis à travers divers domaines nécessaires à la survie de l'organisation. Pour les opérations menées par leurs soldats, attentats ou attaques précises, les organisations doivent financer les véhicules et autres moyens de transport utilisés pour leurs déplacements, l'achat de toutes sortes d'armes, les faux documents d'identité , les frais de subsistance, le matériel médical de base sans compter les commissions du personnel qui transporte les informations ou l'argent liquide à travers les territoires. La propagande et les levées de fonds, vitales pour la pérennité de l'organisation, demandent également un investissement conséquent pour assurer l'accès aux médias sociaux, la création de sites internet dédiés, la publication dans les magazines et journaux ou encore la retransmission des campagnes sur certaines chaînes de télévision et radios. Les formations des nouvelles recrues sont un élément capital pour lequel les organisations investissent dans l'achat de nouvelles armes, d'équipements, de terrains et biens immobiliers servant de camps d'entrainements. Il faut ajouter à cela les salaires et compensations qui seront versées aux membres et à leurs familles. Enfin, de nombreuses organisations terroristes

subventionnent les services de santé, sociaux et éducatifs pour s'assurer ainsi le soutien des populations locales, améliorer leur recrutement et décrédibiliser les gouvernements légitimes (FATF-GAFI, 2015a, pp. 9-10).

En comparaison, le financement des petites cellules terroristes ou des actes isolés, attentat ou départ pour le *djihad*[13], se caractérise par la multiplicité de canaux et de flux financiers de faibles montants – ce que l'on appelle le micro-financement. Le premier exemple est celui des individus radicalisés qui partent aux côtés des organisations terroristes. Ces combattants djihadistes étrangers utilisent des méthodes traditionnelles, généralement l'autofinancement, issu de sources légitimes comme leur salaire, leurs économies ou encore un prêt à la consommation fait quelques jours avant le départ, et parfois de sources illégitimes comme la petite délinquance. Les besoins financiers pour un voyage vers les zones de conflit sont donc minimes et ces mouvements de fonds sont assez difficiles à détecter pour les cellules de renseignements financiers (TRACFIN, 2015, pp. 295-296). L'autre exemple est celui des montants nécessaires pour commettre un acte terroriste isolé. Selon une étude faite par le *Norwegian Defence Research Establishment*, 75% des 40 attaques terroristes extrémistes planifiées – et dans certains cas perpétrées – en Europe entre 1993 et 2013 ont coûté moins de 10 000 dollars aux terroristes (CTIF, 2015b, p.23). Cas plus récents et encore bien présents dans les mémoires, les experts estiment que les attentats de janvier et du 13 novembre 2015 ont nécessité respectivement 25 000 et 80 000 € (BOUTRY et DÉCUGIS, 2018). Ces sommes semblent d'autant plus dérisoires lorsque l'on connaît les conséquences désastreuses d'un attentat tant au niveau humain qu'économique.

2.4. Les tendances en matière de financement du terrorisme en Belgique

En 2018, la CTIF a transmis 47 dossiers en lien avec le financement du terrorisme dont le montant total s'élève à 14 millions d'euros. Elle joue un rôle particulier dans la lutte contre le financement du terrorisme que ces chiffres ne reflètent pas forcément. En effet, ses compétences en matière d'analyse financière lui facilitent l'identification de petits montants, propres au financement du terrorisme, qui malheureusement risquent de passer inaperçus. Sur base de ces transactions financières et de nombreuses informations nationales et internationales mises à sa disposition, la cellule révèle des liens entre certains individus et le financement du terrorisme et met en évidence les réseaux terroristes. (CTIF, 2018, p.22)

Les tendances dans les dossiers relatifs au financement du terrorisme ont quelque peu évolué au cours de ces dernières années. En 2016, ces dossiers concernaient principalement les attentats de Paris perpétrés en 2015 et ceux du 22 mars 2016 à Bruxelles. En 2017, le financement depuis la Belgique des

[13] Guerre sainte

combattants actifs dans les zones de conflit avait été largement analysé et était donc au cœur des dossiers de la CTIF. En 2018, la cellule s'est attardée sur le problème de la radicalisation dans les prisons en commençant par cerner la problématique des paiements effectués en faveur des détenus et travaille, aujourd'hui, en étroite collaboration avec la direction générale des Etablissements pénitentiaires du SPF Justice. (CTIF, 2018, p.22-23)

Au cours de ces dernières années, la Belgique a été exposée à des actions terroristes davantage individuelles qui ont entrainé une augmentation de la vigilance des autorités envers l'extrémisme et le radicalisme. C'est une approche plus proactive dans la lutte anti-terrorisme. Sur le plan financier, celle-ci se traduit par une surveillance accrue des organisations soi-disant humanitaires d'inspiration islamiste. Lorsque ces organisations suspectes sont identifiées, l'identification des donneurs d'ordre permet à la CTIF de renseigner aux autorités un grand nombre d'individus radicalisés mais inconnus de leurs services. (CTIF, 2018, p.23)

La CTIF développe également la problématique des monnaies virtuelles et des nouveaux moyens de paiements utilisés pour financer le terrorisme. Certains dossiers, notamment ceux liés aux attentats de Paris et de Bruxelles, révèlent l'utilisation d'applications mobiles récentes et de systèmes de paiements en ligne par les auteurs et suspects. Outre ces applications donnant une impression de pseudo anonymat, les monnaies virtuelles quant à elles offrent aux terroristes la possibilité d'acheter des armes ou des passeports volés de manière tout à fait anonyme sur le *Dark Web*[14]. Ce réseau est aussi en lien avec la vente de drogue et autres substances illégales, dont les bénéfices pourraient financer le terrorisme. De plus, certains dossiers de la CTIF démontrent que les monnaies virtuelles et les nouveaux moyens de paiements sont utilisés par certaines organisations terroristes pour réaliser des paiements internationaux ou recevoir des dons dans le cadre de campagnes de *crowdfunding*[15] en préservant un anonymat complet. (CTIF, 2018, pp.23-24)

La rapidité d'évolution de ces nouveaux moyens de paiement représente un défi conséquent pour tous les acteurs dans la lutte du financement du terrorisme et requiert une coopération internationale forte et appropriée.

[14] Le terme *Dark Web* fait référence au contenu en ligne crypté accessible uniquement via des logiciels ou navigateurs spécifiques, procurant ainsi l'anonymat à ces utilisateurs. (BLOOMENTHAL, 2019)

[15] Le *crowdfunding*, ou financement participatif, est un mécanisme qui collecte les apports financiers, généralement de petits montants, d'un grand nombre de particuliers au moyen d'une plateforme sur internet en vue de financer un projet. (BOLUZE, 2019)

Chapitre 3 : La lutte au niveau international

3.1. Les principaux acteurs internationaux

Il ne serait pas pertinent dans le cadre limité de cette étude de faire la liste exhaustive de tous les organismes internationaux actifs dans la lutte contre le blanchiment de capitaux et le financement du terrorisme. Nous évoquerons ici les divers acteurs jouant un rôle fondamental sur la scène internationale depuis les premiers actes posés contre ces pratiques jusqu'à aujourd'hui.

3.1.1. L'Organisation de Coopération et Développement Économiques

L'Organisation de Coopération et de Développement Économiques [ci-après OCDE], basée à Paris, compte 36 membres, principalement des pays développés, acteurs principaux sur la scène internationale économique. Jouant essentiellement un rôle d'assemblée consultative, cette organisation internationale a pour mission de promouvoir les différentes politiques favorisant la prospérité et l'égalité des chances en vue d'améliorer le bien-être économique et social à travers le globe (OCDE, 2019a).

Son action repose particulièrement sur la publication de multiples études économiques – analyses, prédictions des tendances et recommandations de politiques économiques – et de nombreuses statistiques. Avec plus de 500 rapports et plus de 5 milliards de données publiés annuellement, l'OCDE est l'une des plus importantes sources de données au monde (OCDE, 2019a).

Dans le cadre de la LBC/FT, l'OCDE compte plusieurs initiatives à son actif telles que la Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales adoptée en 2007, la publication d'un « Manuel de sensibilisation des vérificateurs fiscaux sur le blanchiment de capitaux », l'établissement des listes blanche, grise et noire régulièrement mises à jour mais elle est surtout à l'origine de la création du GAFI (HAAN, pp. 80-81).

3.1.2. Le Groupe d'Action Financière

Le GAFI, en anglais *Financial Action Task Force* [ci-après FATF], a été créé par les États du G7[16] avec leurs partenaires de l'OCDE en 1989 à la suite du sommet de l'Arche à Paris. Cet organisme intergouvernemental s'est fixé pour objectif d'élaborer des politiques de lutte internationale contre le blanchiment de capitaux, le financement du terrorisme, le financement et la prolifération des armes de destruction massive ainsi que de veiller à leur application (FATF-GAFI, 2019b).

[16] Allemagne, Canada, États -Unis, France, Grande-Bretagne, Italie et Japon

Trente ans après sa création, le groupe se compose de 37 pays et territoires et de 2 organisations régionales dont l'Union Européenne (Cf. Annexe 3, Les membres du GAFI). Toutefois, le GAFI a pris conscience qu'une action anti-blanchiment et anti-terrorisme se focalisant uniquement sur ses membres alors que le reste du monde restait sous-règlementé avait un impact très limité. Conscient de cette problématique, le GAFI a décidé de promouvoir l'adoption et la mise en œuvre de ces normes à l'extérieur des frontières du groupe suivant 2 axes :

1) Le réseau de « GAFI régionaux » : mis en place depuis le 1er janvier 2005, celui-ci est formé par différents groupes[17] reconnus comme membres associés du GAFI. Ces derniers s'engagent à respecter et mettre en œuvre les normes établies par le GAFI et à initier un programme de suivi. De cette manière, ils contribuent et renforcent l'engagement mondial dans la LBC/FT.
2) Les juridictions à hauts risques et non coopératives : anciennement appelées « pays et territoires non coopératifs », cette initiative lancée en 1999 avait pour but d'établir une liste de pays et territoires qui n'appliquaient pas suffisamment les normes du GAFI, encourant alors des contre-mesures qui pouvaient aller jusqu'à la suspension des relations financières.

   Aujourd'hui, les juridictions à hauts risques et non coopératives regroupent les différentes juridictions présentant des défaillances stratégiques en matière de LBC/FT. On en dénombre encore quatorze sous la surveillance du GAFI[18] dont deux d'entre elles, l'Iran et la République populaire démocratique de Corée, faisant l'objet d'un appel du GAFI à ses membres et aux autres juridictions à appliquer des contre-mesures (FATF-GAFI, 2019c).

   (KOUTOUNIS et THONY, 2005, pp. 73-75)

Le GAFI est reconnu par la communauté internationale comme l'émetteur des normes en matière de LBC/FT présentées sous forme de recommandations. Publiées pour la première fois en 1990, les 40 recommandations du GAFI portaient essentiellement sur le blanchiment de capitaux lié au trafic de drogue. Elles ont ensuite été révisées en 1996, en 2001 où 9 recommandations spéciales concernant le financement du terrorisme ont été ajoutées suite aux attentats du 11 septembre, en 2003 pour prendre en compte les nouvelles morphologies du blanchiment et dernièrement en 2012, où elles ont été

[17] Membres associés du GAFI actuellement reconnus : Groupe Asie/Pacifique sur le blanchiment de capitaux (GAP), Groupe d'action financière des Caraïbes (GAFIC), Conseil de l'Europe - MONEYVAL (ex PC-R-EV), Groupe Anti-blanchiment de l'Afrique Orientale et Australe (GABAOA), Groupe d'action contre le blanchiment d'argent en Afrique Centrale (GABAC), Groupe d'action financière d'Amérique latine (GAFILAT), Groupe d'Action Financière du Moyen-Orient et de l'Afrique du nord (GAFIMOAN), Groupe Eurasie, Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest (GIABA) (FATF-GAFI, 2019c)

[18] Juridictions actuellement sous surveillance du GAFI : Bahamas, Botswana, Cambodge, Ghana, Iran, Islande, Mongolie, Pakistan, Panama, République populaire démocratique de Corée, Syrie, Trinité-et-Tobago, Yémen, Zimbabwe (FATF-GAFI, 2019c)

complétement refondues sous la forme qu'on leur connaît aujourd'hui, restant ainsi d'actualité et pertinentes. Leur objectif est de définir un cadre complet et cohérent de mesures à mettre en œuvre par les pays du monde entier afin d'améliorer les cadres juridiques nationaux, renforcer les systèmes financiers et développer la coopération internationale pour lutter contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération des armes de destruction massive (Cf. Annexe 1, Les 40 recommandations du GAFI). Elles s'articulent autour des sept catégories suivantes :

A – Politiques et coordination en matière de LBC/FT (recommandations 1 et 2)

B – Blanchiment de capitaux et confiscation (recommandations 3 et 4)

C – Financement du terrorisme et financement de la prolifération (recommandations 5 à 8)

D – Mesures préventives (recommandations 9 à 23)

E – Transparence et bénéficiaires effectifs des personnes morales et constructions juridiques (recommandations 24 et 25)

F – Pouvoirs et responsabilités des autorités compétentes et autres mesures institutionnelles (recommandations 26 à 35)

G – Coopération internationale (recommandations 36 à 40)

Néanmoins, les recommandations du GAFI, prises isolément, ne sont pas contraignantes dans le droit international. Cela n'empêche pas le Groupe de jouer un rôle de leader dans cette lutte d'autant plus que l'application de ses normes est presque devenue un étalon de mesure de l'engagement des différents acteurs. Le caractère international des recommandations du GAFI a également «*le mérite d'empêcher une dispersion trop large des initiatives en fixant un cadre juridique souple mais relativement cohérent* » (HAAN, 2015, p.82).

L'action du GAFI se concentre sur le suivi des progrès réalisés dans la mise en œuvre des recommandations en commençant par ses propres membres. Ce contrôle est effectué selon un double mécanisme : un exercice d'auto-évaluation annuel et un programme d'évaluations mutuelles[19]. Périodiquement, les experts du GAFI estiment le niveau de conformité technique de chaque pays membre en attribuant une notation pour chacune des recommandations[20]. Ces différentes évaluations nationales permettent au GAFI d'identifier et d'étudier les nouvelles tendances et typologies en matière de BC/FT, communiquées dans son rapport annuel, afin de d'adapter la réponse internationale à ces nouvelles menaces (FATF-GAFI, 2019b).

[19] Les équipes d'évaluation sont composées d'experts issus uniquement des pays membres du GAFI, d'où le caractère « mutuel » des évaluations visant à exercer à l'intérieur des groupes une sorte de pression par les pairs.

[20] Il y a quatre notations possibles en matière de conformité technique : conforme (C) ; en grande partie conforme (LC) ; partiellement conforme (PC) ; et non-conforme (NC).

3.1.3. L'Organisation des Nations Unies

Comptant actuellement 193 membres, l'Organisation des Nations Unies [ci-après ONU] est considérée comme l'organisation intergouvernementale la plus importante, la plus puissante et la plus connue au monde chargée de maintenir la paix et la sécurité internationales (ONU, 2019). La Convention de 1998 contre le trafic illicite de stupéfiants et de substances psychotropes, signée à Vienne, est le premier instrument juridique international à incriminer le blanchiment de capitaux issu du trafic de stupéfiants marquant ainsi le début de la contribution des Nations Unis dans la lutte contre ce fléau.

En 1997, elle met en œuvre un Programme mondial contre le blanchiment de l'argent, connu sous l'abréviation GPML, au sein de l'Office des Nations Unies contre la drogue et le crime [ci-après ONUDC] en vue de promouvoir les systèmes de prévention du blanchiment sur le plan législatif, administratif et judiciaire. Ce programme accompagne les différentes règles mises en place par les conventions des Nations Unies, en particulier celle de Palerme contre la criminalité transnationale organisée, ratifiée en novembre 2000, ainsi que celle contre la corruption, ratifiée en octobre 2003. Ces conventions élargissent la portée de l'infraction de blanchiment d'argent mais exhortent également les états à créer un régime national complet de surveillance et de règlementation ainsi que des cellules de renseignements financiers [ci-après CRF]. En outre, il faut ajouter la Convention internationale pour la répression du financement du terrorisme, entrée en vigueur en avril 2002, obligeant les États membres à prendre des mesures pour protéger leurs systèmes financiers contre le financement du terrorisme. L'ONU soutient également le GAFI depuis 2005 à travers deux résolutions en soulignant l'importance de la mise en œuvre de ses 40 recommandations (ONUDC, 2019a).

Aujourd'hui, l'ONUDC est très active dans l'assistance technique aux autorités des pays en développement, l'organisation de formations sous forme d'ateliers ou d'e-learning. Elle fournit également diverses stratégies de lutte contre le blanchiment et conseille sur l'amélioration des politiques bancaires (ONUDC, 2019b).

3.1.4. Le Fonds Monétaire International et la Banque Mondiale

Créés en 1944 lors de la Conférence de Bretton Woods, le Groupe de la Banque Mondiale[21] et le Fonds Monétaire International [ci-après FMI] regroupent chacun 189 membres. La mission du FMI est

[21] Composition du Groupe : la Banque internationale pour la reconstruction et le développement (BIRD), l'Association internationale de développement (IDA), la Société financière internationale (IFC), l'Agence multilatérale de garantie des investissements (MIGA), le Centre international pour le règlement des différends relatifs aux investissements (CIRDI)

principalement d'assurer la stabilité du système monétaire international et de gérer les crises monétaires et financières en procurant des crédits aux pays en difficulté financière. Le Groupe de la Banque Mondiale fournit également des aides, des financements et des conseils à ses membres mais se concentre sur les pays en développement pour réduire la pauvreté et améliorer la prospérité (BANQUE MONDIALE, 2019).

Comme expliqué précédemment, le blanchiment de capitaux et le financement du terrorisme exposent la stabilité et l'intégrité du système financier à des risques considérables. Les pays en voie de développement présentant des faiblesses au niveau de leur dispositif LBC/FT sont des cibles très convoitées par les organisations criminelles. C'est pourquoi depuis 2001, la lutte contre le blanchiment et le financement du terrorisme ont été ajoutées au Programme d'évaluation du secteur financier, en anglais *Financial Sector Assessment Program*, lancé par les deux institutions financières internationales offrant aux États une évaluation de l'intégrité de leur système financier et une assistance technique pour améliorer celui-ci. Le FMI, la Banque Mondiale ainsi que le GAFI ont élaboré une méthodologie commune pour évaluer la conformité des pays avec les standards internationaux de LBC/FT consacrant ainsi plus de 250 normes internationales. En plus de la réalisation de ces nombreuses évaluations, le FMI a également lancé un fond fiduciaire pour financier l'assistance technique dans le domaine de la LBC/FT et il analyse régulièrement les conséquences économiques des questions d'actualité telles que la monnaie virtuelle ou la diminution des relations de correspondances bancaires. (HAAN, 2015, pp.89-93)

3.2. L'Union Européenne et ses directives

Le 8 novembre 1990, le Conseil de l'Europe [ci-après COE] ratifie la Convention de Strasbourg relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime, marquant le début de l'engagement européen dans la lutte contre le blanchiment de capitaux. L'Union Européenne, dont l'objectif est de protéger son marché intérieur de toute criminalité et d'assurer une croissance économique équilibrée, s'est calquée sur ce mouvement en adoptant par la suite plusieurs directives dans le domaine de la lutte contre le blanchiment d'argent et le financement du terrorisme.

Les directives européennes sont des actes législatifs qui fixent des objectifs à tous les pays de l'Union Européenne tout en leur laissant la liberté d'élaborer leurs propres mesures pour les atteindre. Cet instrument juridique contraignant permet de transposer les recommandations du GAFI, normes internationales en matière LBC/FT, dans la législation de chaque état adhérent de manière à harmoniser les législations nationales des pays européens (EUROPA, 2019). À ce jour, 5 directives relatives au domaine de la LBC/FT ont été approuvées.

La première directive relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux (91/308/CEE) a été publiée le 10 juin 1991. Première étape au niveau de l'Union européenne dans la LBC/FT, elle est considérée comme le texte fondateur de la mise en œuvre du volet préventif de la lutte anti-blanchiment. Elle astreint les établissements de crédit à identifier leurs clients en demandant la documentation appropriée, à mettre en place un processus de contrôle interne garantissant un programme de lutte adapté et à signaler les indications de blanchiment aux autorités compétentes. La directive impose également une coopération internationale pour assurer l'efficacité de ces mesures.

Quelques mois après les attentats du 11 septembre, cette première directive est modifiée par la directive 2001/97/CE du 4 décembre 2001 pour adapter le dispositif européen aux nouvelles pratiques criminelles et à la mise à jour des recommandations du GAFI. L'avancée majeure de cette seconde directive est l'élargissement de son champ d'application puisque les infractions sous-jacentes ne sont plus uniquement liées au trafic de stupéfiants et que désormais les obligations incombent également aux professions non financières qui représentent des secteurs risqués comme les notaires et avocats, les agences immobilières, ou encore les comptables et conseillers fiscaux. Cette directive insiste également sur le besoin de vigilance accrue lors de l'identification des clients mais aussi des bénéficiaires effectifs[22] et des mandataires lors de la relation d'affaires.

La troisième directive anti-blanchiment, la directive 2005/60/CE du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, abroge et remplace la directive 91/308/CEE modifiée par la directive 2001/97/CE. Comme son nom l'indique, l'objectif de cette troisième directive s'élargit pour inclure la lutte contre le financement du terrorisme. Elle éclaire certains points restés flous dans la directive précédente comme les procédures d'identification du client, la notion de bénéficiaire effectif, la notion de devoir de vigilance à l'égard de la clientèle ou encore le niveau de surveillance à appliquer lors des transactions en espèces. En outre, elle renforce les obligations concernant la mise en place de CRF au niveau national en vue d'améliorer l'efficacité du système LBC/FT et la collaboration internationale.

Suite aux modifications des recommandations du GAFI qui ont eu lieu en 2012, une harmonisation de la législation européenne était indispensable. La quatrième directive européenne,

[22] « […] *Personnes physiques qui, en dernier ressort, possèdent ou contrôlent le client, le mandataire du client ou le bénéficiaire des contrats d'assurance-vie, et/ou la ou les personnes physiques pour lesquelles une opération est exécutée ou une relation d'affaires nouée* […]. (Loi du 18 septembre 2017, Art.4, § 27)

actuellement d'application, est la directive 2015/849 du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. Le champ d'application est encore élargi en intégrant l'entièreté du secteur des jeux d'argent et de hasard ainsi que les personnes exerçant une activité financière à titre occasionnel. Elle améliore aussi les dispositions concernant l'identification des bénéficiaires effectifs et en ajoute concernant les PPE. Cette directive marque également l'introduction de l'approche fondée sur les risques dans le dispositif préventif LBC/FT. Au niveau de la lutte contre le financement du terrorisme, elle renforce le pouvoir des CRF européennes en vue de faciliter leur coopération et applique une surveillance plus sévère aux pays à risque en matière d'activités terroristes.

Récemment approuvée, la directive 2018/843 du 30 mai 2018 modifie la directive 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. Le champ d'application de cette dernière est encore élargi pour prendre en compte les acteurs du marché des crypto-monnaies[23] dans la liste des personnes assujetties. Les mesures à l'égard des clients établis dans les pays tiers à risque sont encore renforcées tout comme les mesures de vigilance à l'égard de la clientèle. La cinquième directive porte également une attention particulière à la mise en place du registre des bénéficiaires effectifs par les entreprises assujetties, sa mise à jour régulière et l'amélioration de son accessibilité.

La mise à jour périodique de ces Directives permet de prendre en compte « *la nature changeante du blanchiment de capitaux et du financement du terrorisme – d'autant plus changeante que la technologie et les moyens à la disposition des criminels évoluent constamment* – (qui) *impose d'adapter en permanence le cadre juridique devant permettre de contrer ces menaces* » (COMMMISSION EUROPEENNE, 2013, p.2). Une des évolutions observées dans ces actes législatifs est le renforcement progressif vers une prévention basée sur les risques qui aboutit finalement sur la consécration de l'approche fondée sur les risques comme principe directeur. Non seulement ces Directives harmonisent les législations nationales et les dispositifs de LBC/FT des pays membres de l'Union Européenne mais elles favorisent aussi la coopération entre ceux-ci et avec le reste du monde, élément fondamental dans la réussite des dispositifs LBC/FT.

[23] Moyen de paiement numérique utilisable sur un réseau informatique décentralisé de pair à pair, les crypto-monnaies sécurisent leurs transactions en s'appuyant sur les principes de la cryptographie de haut niveau et incorporent l'utilisateur dans les processus d'émission et de règlement des transactions. (PAIANO, 2018)

3.3. Le développement de la coopération internationale

Dès 1990, les pays ont été forcés de constater que le système mis en place dans la LBC/FT exigeait une nouvelle structure permettant de faire le lien entre les acteurs du secteur privé – pouvant détecter et signaler les transactions financières suspectes – et les acteurs de la justice pénale – accrédités pour enquêter sur ces transactions et potentiellement appliquer les sanctions nécessaires en cas de délit. Prenant en compte ces considérations, des entités nationales spécialisées ont donc été mises en place dans les différents États : les cellules de renseignements financiers. Elles sont principalement chargées de recevoir, analyser et transmettre les déclarations de soupçon identifié et signalé par le secteur privé aux autorités pénales compétentes. L'avantage de ces cellules se trouve dans les nombreuses sources d'informations financières mises à leur disposition entrainant une meilleure analyse et une évaluation plus poussée des déclarations de soupçon reçues. (COE, 2019)

En tant qu'instrument de coordination internationale, les cellules de renseignements financiers ont la capacité de coopérer à la fois avec leurs homologues étrangers et avec d'autres institutions nationales pour échanger des renseignements. Créé en 1995, le groupe Egmont unit 164 CRF et constitue aujourd'hui la référence internationale pour l'échange d'informations de nature financières, bancaires et fiscales. Il a mis en place un certain nombre de normes clé que les CRF doivent respecter pour optimiser les interactions et les échanges de renseignements ainsi qu'un site internet sécurisé, appelé Egmont Secure Web, canal largement utilisé par les membres du groupe pour les transferts d'informations. (EGMONT GROUP, 2019)

Ces mécanismes d'échange d'informations internationaux sont essentiels au vu du caractère transfrontalier des délits de blanchiment de capitaux et de financement du terrorisme. Toutefois, il est important de souligner que cette coopération internationale reste conditionnée, notamment par le principe de réciprocité et celui de l'autorisation à la dissémination de l'information.

Le premier implique « *qu'une CRF ne peut pas solliciter de son homologue étranger ce qu'elle-même ne serait pas en mesure de lui communiquer si le sens était inversé* ». Concrètement, cela signifie qu'une CRF doit non seulement connaître le statut et les compétences de la CRF étrangère avec qui elle désirerait échanger des informations mais aussi partager les mêmes prérogatives que celle-ci pour s'assurer une réponse complète à sa requête. (PEREIRA, 2011, p.70)

L'échange d'informations est également soumis au principe de l'autorisation à la dissémination de l'information. L'application de celui-ci peut s'expliquer comme suit : « *si la CRF destinataire de l'information sur le soupçon étranger souhaite communiquer et/ou disséminer l'information reçue d'une autre CRF aux autorités de son pays, elle doit solliciter par écrit une autorisation à la CRF qui lui a*

communiqué l'information ». En pratique, si la CRF ayant communiqué l'information refuse que l'information soit effectivement transmise aux autorités compétentes du pays demandeur, ces informations deviennent inutilisables dans les dossiers officiels des CRF pouvant être transmis aux autorités pénales. (PEREIRA, 2011, pp.70-71)

Ces conditions révèlent finalement certaines failles dans le système de coopération internationale, particulièrement concernant les échanges d'informations relatives aux déclarations de soupçon de blanchiment ou de financement de terrorisme. Elles mettent également en évidence la nécessité toujours croissante de réduire les disparités entre les différentes législations pour améliorer le dispositif préventif LBC/FT.

Chapitre 4 : La lutte au niveau belge

4.1. La politique à deux volets du système de LBC/FT en Belgique

Inspiré des normes internationales, le dispositif belge LBC/FT combine deux approches complémentaires qui viennent structurer ce que l'on appelle la chaîne LBC/FT. Cette chaîne débute avec un volet préventif, visant la détection et le signalement des transactions financières suspectes engageant les acteurs privés comme premier maillon de la chaîne, suivi par un volet répressif, impliquant les sanctions pénales appliquées par les autorités compétentes en cas d'infraction.

4.1.1. Le volet préventif

L'objectif général du dispositif préventif de la LBC/FT est de préserver l'économie légale de l'introduction de fonds provenant d'activités illicites en évitant ainsi le développement des conditions favorables à l'infraction de blanchiment, et de détecter les transactions destinées au financement du terrorisme (BAUDRIHAYE-GÉRARD et CARDON, 2018, pp.1-2).

Ce volet préventif n'a cessé de faire l'objet de renforcements normatifs ces dernières années notamment avec la révision complète des recommandations du GAFI en 2012 puis avec la publication de la 4ème Directive *AML* de l'UE en 2015, devant être transposée en droit national pour le 26 juin 2017. C'est dans cette optique que le législateur fédéral belge a élaboré une nouvelle loi en la matière : la Loi 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, entrée en vigueur le 16 octobre 2017.

Cette loi représente le fondement principal de l'approche préventive de la LBC/FT. Elle liste tout d'abord les organismes et catégories de personnes concernées puis définit les obligations en matière de prévention du blanchiment de capitaux et du financement du terrorisme de ces entités assujetties. Celles-ci se composent de l'obligation d'organisation et de contrôle interne, l'obligation d'évaluation globale des risques, l'obligation de vigilance à l'égard de la clientèle et des opérations et finalement de l'obligation de déclaration des opérations suspectes. Elles sont interdépendantes et chacune d'entre elles constitue une composante du mécanisme global de prévention. Quant à l'ensemble du mécanisme, il doit satisfaire les obligations en matière de communication, de conservation et de protection des données. Le non-respect de ces différentes obligations par les personnes et organismes concernés peut se voir sanctionner par des amendes administratives ou pénales en fonction de la gravité de l'infraction. (MEES, 2017)

Par rapport à la législation précédente[24], la Loi du 18 septembre 2017 consacre l'approche fondée sur les risques (Cf. Chapitre 5) et introduit un système de procédure « en cascade » pour l'identification et l'évaluation des risques qui s'effectue dès lors au niveau supranational par la Commission européenne, au niveau national par les États membres et au niveau des entités assujetties.

Enfin, la loi prévoit des mesures de collaboration nationales et internationales entre les autorités compétentes et définit également leur champ d'action. C'est le cas notamment pour la Cellule de Traitement des Informations Financières, cellule belge de renseignements financiers, pour laquelle son rôle, les responsabilités et les tâches en matière d'analyse opérationnelle et stratégique sont davantage détaillés dans cette nouvelle législation.

4.1.2. Le volet répressif

Dernier maillon de chaîne LBC/FT, les acteurs de la justice pénale interviennent dans le cadre du volet répressif en incriminant l'infraction de blanchiment et de financement du terrorisme au moyen des régimes d'enquête, de saisie, de confiscation et de condamnation.

Le volet répressif belge se base sur deux articles du Code pénal, l'article 505 relatif à l'infraction de blanchiment de capitaux et l'article 140 relatif à l'infraction de financement du terrorisme.

L'article 505 sous sa forme actuelle consacre le blanchiment comme infraction autonome, c'est-à-dire qu'elle est punissable indépendamment de l'infraction sous-jacente de laquelle proviennent les capitaux, la rendant ainsi plus facile à condamner. En outre, il sanctionne l'ensemble des personnes qui sont intervenues dans le processus du blanchiment puisqu'il punit la dissimulation mais également la gestion des biens ayant une origine illicite. Les blanchisseurs encourent jusqu'à 100 000 euros d'amende et risquent entre quinze jours à cinq ans de prison uniquement pour l'infraction de blanchiment. La mention de l'article 42 du Code pénal relative à la confiscation spéciale en cas de crime ou de délit permet de geler les biens concernés par le blanchiment et ainsi freiner ce phénomène.

L'article 140 condamne toutes formes de participation à un groupe terroriste en supposant que le préposé ait eu ou aurait dû avoir connaissance que cette participation pourrait contribuer à commettre un crime ou un délit du groupe terroriste. Cette participation est passible d'une durée d'emprisonnement entre cinq à dix ans et d'une amende de cent à cinq mille euros.

Toutefois, ce travail, qui ne se veut pas juridique, ne développera pas plus en profondeur la partie répressive du cadre règlementaire belge en matière de LBC/FT.

[24] Loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme

A la fin de cette section, il est intéressant de se pencher sur la relation de dépendance établie entre ces deux volets. Lorsqu'une entité assujettie suspecte un tiers d'infraction, elle fait ce que l'on appelle une déclaration de soupçon à la CTIF (Cf. Annexe 4, Le formulaire de déclaration de soupçon). La cellule procède ensuite à l'analyse de cette déclaration et si elle estime que le soupçon est justifié, elle transmet un dossier aux autorités pénales compétentes. Par conséquent, le fonctionnement du dispositif de LBC/FT tel que nous le connaissons aujourd'hui amène une certaine dépendance du système répressif au regard du dispositif préventif puisqu'une part dominante des condamnations prononcées en matière de BC/FT émanera des dossiers transmis au préalable par la CTIF (FORIR, 2018, pp. 21-26). La CTIF joue donc le rôle de maillon central dans le dispositif belge.

4.2. La Cellule de Traitement des Informations Financières

Comme le préconisait l'UE, dès 1993 la Belgique a mis en place sa propre cellule de renseignements financiers en créant un nouvel organisme, la CTIF. Elle a pour mission d'analyser et d'enrichir les informations reçues de la part des tous les organismes et personnes visés par la Loi et le cas échéant, de transmettre celles-ci aux autorités judiciaires. Composée d'un officier supérieur détaché de la police fédérale, d'experts en matière financière et placée sous le contrôle d'un magistrat, la cellule réunit les représentants de la justice et ceux du secteur financier, compromis nécessaire au bon fonctionnement du système de LBC/FT en Belgique (CTIF, 2019). Le schéma ci-dessous résume la procédure mise en place lors de présomption de blanchiment de capitaux ou de financement du terrorisme :

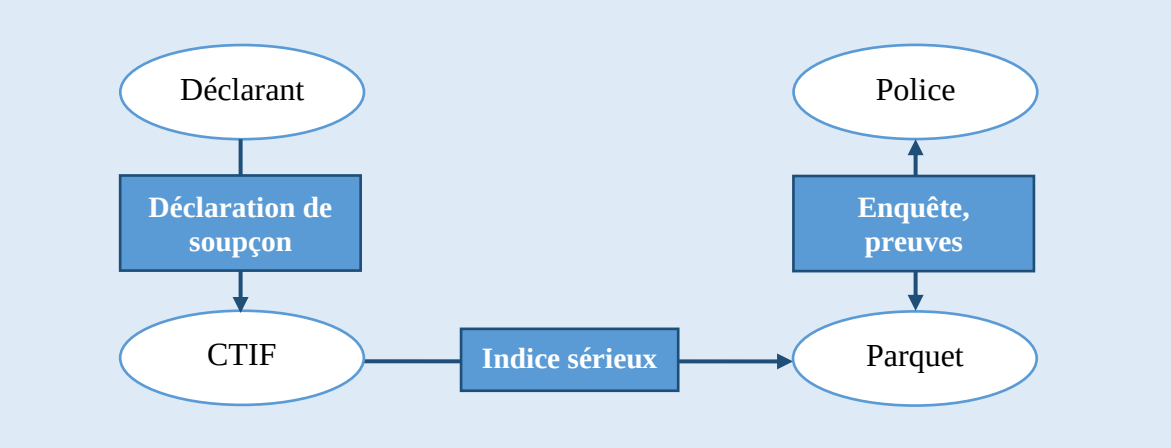


Figure 4.1 : Procédure en cas de présomption de blanchiment de capitaux ou de financement du terrorisme
Source : BRAUX, 2015, p.30

La CRF belge fonctionne selon un modèle administratif consacrant son indépendance à l'égard du pouvoir judiciaire. En effet, la CTIF possède son propre budget et se définit comme étant « *une autorité administrative indépendante, dotée de la personnalité juridique, qui est chargée du traitement*

et de la transmission d'informations, en vue de la lutte contre le blanchiment de capitaux et le financement du terrorisme […] ». Cette indépendance formelle place la CTIF dans le rôle d'intermédiaire entre les institutions financières et les services d'enquêtes et permet d'éviter que les informations transmises soient utilisées à d'autres fins, d'autant plus que les membres de ces services sont « *soumis à un secret professionnel très strict* » (CTIF, 2019). L'objectif de cette confidentialité est de protéger les déclarants en conservant leur anonymat – la déclaration de soupçon n'est jamais transmise aux autorités judiciaires par respect de l'article 59 de la Loi – afin de favoriser leur coopération avec la cellule. Ils sont également protégés par l'article 57 de la Loi qui stipule premièrement qu'une divulgation d'informations effectuée de bonne foi[25] ne constitue pas une violation d'une quelconque restriction à la divulgation d'informations imposée par un contrat et que cette déclaration ne peut entraîner aucune mesure préjudiciable ou discriminatoire en matière d'emploi. Deuxièmement, l'article précise que cette immunité reste acquise même dans le cas où le déclarant n'avait pas une connaissance précise et certaine de l'activité criminelle sous-jacente et même dans le cas où, après une analyse approfondie, aucune activité illicite n'était liée à l'opération déclarée à la CTIF. Ces mesures de protection envers les déclarants sont vitales compte tenu de la condition de la CTIF, qui est en situation de dépendance informationnelle à l'égard des déclarants (BAUDRIHAYE-GÉRARD et CARDON, 2018, pp.4-6).

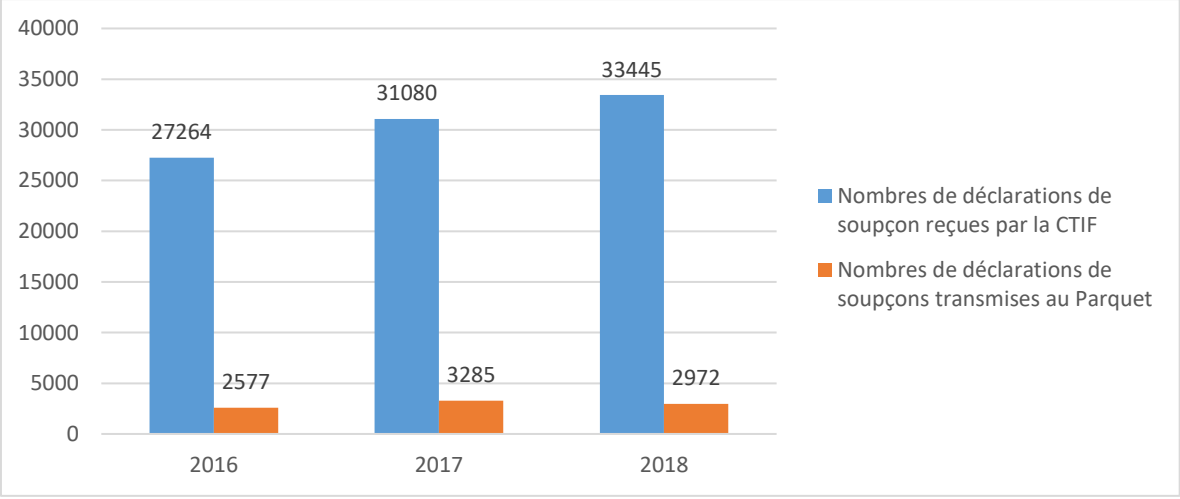
En effet, bien que certains déclarants aient l'obligation de transmettre des déclarations « automatiques » basées sur des critères objectifs comme le montant des transactions, les déclarations sur la base du soupçon sont, selon les acteurs de la CTIF, beaucoup plus pertinentes. Ils estiment que le premier filtre exercé par le déclarant leur permet de commencer directement à « essayer de confirmer le soupçon du déclarant ». Pour aider les déclarants dans leurs obligations et améliorer leur travail de repérage des soupçons, la Cellule s'est investie de manière proactive depuis quelques années déjà à travers la publication d'un rapport annuel envoyé à tous les assujettis. Elle a également mis en place un processus de *feedbacks* individuels sur la base des informations et documents transmis. Cette dépendance de la CTIF envers les déclarants peut poser problème lorsque les institutions financières, divisées entre obligations légales et objectifs commerciaux, décident de faire des « déclarations couverture[26] », tardives et/ou incomplètes avec comme seul but une protection contre des poursuites

[25] C'est-à-dire que la déclaration n'est pas effectuée dans le but de nuire, qu'elle ne se base pas sur des informations que le déclarant savait erronées et qu'elle ne présente pas de manquement à l'obligation d'examen attentif. (Loi du 18 septembre 2017, Article 57)

[26] Déclarations effectuées pour chacune des opérations exécutées par un client pour lequel une déclaration a déjà été faite. Elles sont transmises de manière systématique par les entités assujetties, même en l'absence de tout soupçon. (FATF-GAFI, 2015b, p.53)

éventuelles. Toutefois, malgré la fragilité de cette position, le système subjectif présente un intérêt particulier pour la CTIF puisqu'il lui permet de réguler correctement le nombre de déclarations entrantes mais également de maintenir la part d'analyse et de recherche qui lui est propre dans le système de LCB/FT. (BAUDRIHAYE-GÉRARD et CARDON, 2018, pp.6-13)

Lorsqu'une déclaration de soupçon est transmise à la cellule, elle fait l'objet d'un travail d'enquête. La CTIF a à sa disposition une multitude de canaux d'information et de coopération permettant d'analyser et d'enrichir les soupçons des déclarants. Ces renseignements peuvent être fournis par les CRF étrangères au moyen de plateformes dédiées telles que le *Egmont Secure Web* au niveau mondial ou le « FIU.net » au niveau européen. Au niveau national, la CTIF collabore avec la police, le parquet fédéral, les services de renseignements civils et militaires ou encore l'Organe de Coordination pour l'Analyse de la Menace [ci-après OCAM] dans le cadre du financement du terrorisme (CTIF, 2019). Pour pouvoir transmettre un dossier au procureur du Roi ou au procureur fédéral, la cellule doit avoir identifié un « indice sérieux » d'infraction de blanchiment ou de financement du terrorisme. Par conséquent, l'enquête de la CTIF constitue un deuxième filtre dans le dispositif de LBC/FT et évite ainsi d'inonder les parquets. Le graphique ci-dessous donne un aperçu du nombre de déclarations traitées chaque année par la Cellule ainsi que du nombre de déclarations effectivement transmises aux autorités judiciaires[27]. Nous analyserons plus en détails le traitement de ces déclarations par la CTIF et les autorités judiciaires au cours de la deuxième partie de cette étude (Cf. Chapitre 8, Les enjeux actuels)



Graphique 4.1 : Ventilation des déclarations de soupçon reçues et transmises par la CTIF aux autorités judiciaires pour les années 2016, 2017 et 2018

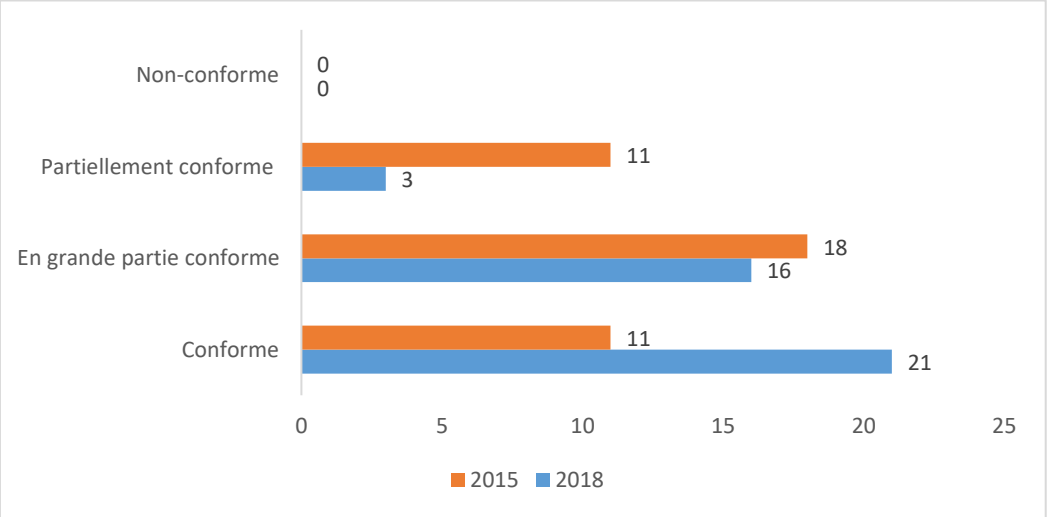
Source : CTIF, 2018, pp.40-42

[27] Pour protéger les déclarants, la CTIF ne transmet pas de copie des déclarations de soupçon mais uniquement les éléments relatifs aux opérations suspectes que celles-ci contiennent, enrichis de son analyse. (CTIF, 2018, p.40)

4.3. Les rapports d'évaluation mutuelle du GAFI

Comme expliqué précédemment, le GAFI évalue la conformité technique de chacun de ses membres de façon périodique. La dernière évaluation mutuelle de la Belgique a été menée en 2014 où une équipe d'experts s'est rendue sur place pour une analyse complète du dispositif de LBC/FT au regard des 40 recommandations du GAFI. Ces évaluations rendent compte de la position de la Belgique par rapport à ses homologues internationaux et mettent en lumière les points forts de son dispositif ainsi que les mesures à mettre en place pour l'améliorer. Le quatrième rapport d'évaluation mutuelle de la Belgique en matière de LBC/FT a été approuvé par le GAFI en février 2015. La Belgique, ayant renforcé ses mesures de lutte, particulièrement au travers de la Loi du 18 septembre 2017, a fait l'objet d'un rapport de suivi publié le 3 septembre 2018. (CTIF, 2019)

Ce rapport de suivi renforcé analyse les progrès de la Belgique uniquement par rapport aux lacunes de conformité techniques qui avaient été détectées auparavant dans son rapport d'évaluation mutuelle de 2015. Pour chacune des recommandations du GAFI, une notation avait été attribuée, celle-ci pouvant aller de « conforme », « en grande partie conforme », « partiellement conforme » jusqu'au seuil critique de « non-conforme ». Entre 2015 et 2018, les notes attribuées par le GAFI à certaines recommandations ont été rehaussées comme l'atteste ce graphique :



Graphique 4.3 : Notations de conformité technique accordées à la Belgique par le GAFI dans son REM en avril 2015 et dans son rapport de suivi en septembre 2018
Source : FATF-GAFI, 2018, p.1 et p.21

Ce rehaussement est caractérisé par une diminution des recommandations qui étaient évaluées « partiellement conforme » et une forte augmentation des recommandations notées « conforme ».

Toutefois, les recommandations 6, 7 et 13 (Cf. Annexe 1, Les 40 recommandations du GAFI) obtiennent encore la note « Partiellement conforme ». Les recommandations 6 et 7 concernent les

sanctions financières ciblées liées respectivement au terrorisme et à son financement ainsi qu'à la prolifération des armes de destruction massive. Selon les notes interprétatives de ces deux recommandations, les sanctions financières telles que le gel des fonds ou autres biens doivent pouvoir s'appliquer « *sans délai* », c'est-à-dire en quelques heures (FATF-GAFI, 2018, pp.40-48). Les experts du Groupe maintiennent cette notation parce qu'actuellement, les sanctions financières mentionnées dans ces deux recommandations ne sont toujours pas appliquées sans délai compte tenu du fait que le processus décisionnel belge peut durer de 2 à 4 jours. La 13ème recommandation du Groupe porte sur l'obligation de déclaration de soupçon émanant des institutions financières. Sa lacune principale se trouve dans les mesures de vigilance spécifiques requises en matière de correspondance bancaire transfrontalière qui, en Belgique, ne s'appliquent pas dans les relations avec les institutions financières de l'Espace économique européen (FATF-GAFI, 2018).

Dans l'ensemble, la Belgique est un bon élève puisque plus de la moitié des 40 recommandations obtiennent la notation maximale. Elle a réalisé d'importants progrès pour combler les lacunes de conformité technique mises en avant en 2015 et cette évolution se marque à travers l'amélioration des ratings de 15 recommandations.

Chapitre 5 : L'approche fondée sur les risques

5.1. L'objectif de l'approche fondée sur les risques

Les risques d'exposition au blanchiment d'argent et au financement du terrorisme sont multiples et différents pour chacune des entités assujetties. Ils dépendent des caractéristiques de la clientèle, de la nature des produits ou services proposés par les entités, des zones géographiques dans lesquelles elles opèrent, de leurs canaux de distribution ou encore des lois et règlements auxquels elles sont soumises (BNB, 2019). Dans le cadre de la LBC/FT, il est primordial que chaque acteur comprenne les risques auxquels il est exposé pour pouvoir ensuite appliquer des mesures pertinentes et atténuer ces risques.

C'est dans cette optique qu'en 2012, la 1ère recommandation du GAFI a consacré l'approche fondée sur les risques, en anglais *risk based approach* [ci-après RBA], en la désignant comme le fondement essentiel du dispositif LBC/FT de chaque membre (Cf. Annexe 1, Les 40 recommandations du GAFI). Pour justifier le choix de cette nouvelle méthode d'évaluation des risques, le GAFI précise :

> *« Les normes du GAFI ont également été revues afin de renforcer les obligations dans les situations de risque plus élevé et de permettre aux pays d'adopter une approche plus ciblée dans les domaines présentant des risques élevés et dans les domaines où la mise en œuvre pourrait être renforcée. Les pays devraient d'abord identifier, évaluer et comprendre les risques de blanchiment de capitaux et de financement du terrorisme auxquels ils sont confrontés, puis adopter des mesures appropriées pour atténuer ces risques. L'approche fondée sur les risques permet aux pays, dans le cadre des obligations du GAFI, d'adopter un ensemble de mesures plus souples, afin d'allouer leurs ressources de manière plus efficace et d'appliquer des mesures préventives proportionnelles à la nature des risques dans le but d'optimiser leurs efforts. »*
> (FATF-GAFI, 2012, p.7)

Concrètement, le but de cette approche est d'adapter les mesures de prévention contre le blanchiment de capitaux et le financement du terrorisme en fonction des risques auxquels les institutions sont exposées. Si des personnes ou organismes présentent un risque faible de par leur nature ou leur ampleur, les États peuvent décider d'assoupir leurs dispositions de LBC/FT voire même de les en exempter complètement. À l'inverse, lorsque le degré de risque présenté est plus élevé, les mesures de protection devront être renforcées. Pour ce faire, les États doivent donc mettre en place une procédure d'évaluation des risques de BC/FT.

Il est important de souligner que, aussi intelligente soit-elle, l'approche fondée sur les risques n'est pas infaillible. Il peut arriver qu'une institution ait pris toutes les mesures raisonnables pour

identifier et atténuer les risques BC/FT, mais être tout de même utilisée à des fins de blanchiment ou de financement du terrorisme (FATF-GAFI, 2014, p.6). Néanmoins, cette nouvelle approche instaurée par le GAFI offre une amélioration dans la gestion des risques liés au BC/FT, une meilleure allocation des ressources investies dans cette lutte, une concentration des institutions sur les menaces identifiées comme réelles et surtout une nouvelle flexibilité d'adaptation aux risques qui évoluent plus vite que les différentes législations. (NÉLIS, 2017, p.41).

Également renforcée dans la 4ème directive européenne, la mise en place de l'approche fondée sur les risques a été transposée en droit national par la Loi du 18 septembre 2017 pour aider les institutions à gérer efficacement les risques de BC/FT identifiés au niveau de l'Union européenne, de la Belgique et de l'institution.

5.2. La pyramide de gestion des risques de BC/FT

Comme l'indique le GAFI, les évaluations des risques de BC/FT devraient être entreprises à différents niveaux avec des objectifs et une portée différents. Dans ce sens, le groupe entend une évaluation supranationale qui regroupe plusieurs pays, une évaluation nationale à l'échelle du pays et enfin une évaluation infranationale qui s'effectue par exemple par secteur, par région ou pour une fonction opérationnelle particulière dans un pays (FATF-GAFI, 2013, pp.10-11). L'Union Européenne a complétement intégré cette vision pyramidale en créant, au travers de la 4ème directive anti-blanchiment, un processus d'identification et d'évaluation des risques « en cascade ».

5.2.1. Niveau supranational : la Commission Européenne

À la tête de cette pyramide, nous retrouvons bien entendu les organismes internationaux, tels que le GAFI ou le FMI. Néanmoins, c'est bel et bien l'Union Européenne qui a rendu les différentes normes LBC/FT contraignantes pour ses États membres.

L'article 6 de la quatrième directive anti-blanchiment charge la Commission européenne de réaliser un rapport qui traite des risques de BC/FT pesant sur le marché intérieur et liés à des activités transfrontières. Ce rapport fait office d'évaluation supranationale au niveau de l'Union et doit être mis à jour tous les deux ans ou plus fréquemment si nécessaire. Après la publication d'un premier rapport en juin 2017, la Commission a récemment partagé une seconde évaluation en juillet 2019. Elle met en lumière les secteurs, produits et services particulièrement exposés à des risques BC/FT, les vulnérabilités spécifiques recensées au niveau de l'UE et fournit des recommandations à l'adresse des États membres. (COMMISSION EUROPEENNE, 2019)

En plus de ces rapports, la 4ème directive apporte également une ligne directrice à laquelle les États membres doivent se conformer dans leur évaluation nationale. L'Union harmonise ainsi l'approche fondée sur les risques en imposant des facteurs indicatifs de situations de risque selon trois critères centraux : les facteurs inhérents aux clients, les facteurs liés aux produits, services, transactions ou canaux de distribution et les facteurs de risque géographiques. (VAN COILE et VANDERSTICHELEN, 2015)

5.2.2. Niveau national : les États membres

Tout en s'appuyant sur les directives et circulaires de l'UE, chaque État membre doit lui aussi prendre des mesures appropriées pour identifier, évaluer et atténuer les risques de BC/FT auquel il est confronté. Par ailleurs, l'évaluation nationale des risques, réalisée de façon périodique, doit être mise à disposition des autres États membres, de la Commission européenne et des autorités européennes de surveillance. Pour réaliser au mieux cette mission, les États sont tenus de désigner une autorité chargée de coordonner la réponse nationale à ces risques et d'informer les entités assujetties lorsque des mesures de vigilance particulières doivent être adoptées. (Directive UE 2015/849, Art.7)

En Belgique, la réalisation de l'évaluation des risques liés au blanchiment de capitaux a été confiée au Comité ministériel de coordination de la lutte contre le blanchiment de capitaux d'origine illicite. Cet organe établit et coordonne la politique générale de la lutte anti-blanchiment en déterminant, par exemple, les priorités des services concernés par cette lutte. Au sujet de la lutte contre le financement du terrorisme, c'est au Conseil national de sécurité qu'il revient de réaliser l'évaluation des risques liés au financement du terrorisme et la prolifération des armes de destruction massive. (Loi du 18 septembre 2017, Art.4, 68-69)

5.2.3. Niveau infranational : les entités assujetties

Lorsque l'on descend encore plus bas dans les échelons de la « grande chaîne de LBC/FT », nous arrivons au niveau des entités assujetties. Finalement, la mise en œuvre de l'approche fondée sur les risques repose en grande partie sur ces entités qui sont les premières exposées aux risques de BC/FT. C'est dans cette optique que l'UE demande à ses États membres de veiller à ce que les entités assujetties prennent des mesures de prévention appropriées en tenant compte néanmoins des documents, rapports et informations recueillies ou reçues par les échelons supérieurs. (Directive UE 2015/849, Art.8)

La Loi du 18 septembre 2017 a transposé cette exigence envers les entités assujetties dans l'obligation de réaliser une évaluation des risques de BC/FT à un double niveau.

Premièrement, les entités assujetties sont tenues de prendre des mesures appropriées et proportionnées à leur nature et à leur taille pour identifier les risques BC/FT auxquelles elles sont

exposées. Une fois cette évaluation globale des risques réalisée, elles mettent alors en place diverses politiques, procédures et mesures de contrôle internes appropriées pour faire face aux risques BC/FT identifiés. Ainsi, l'approche fondée sur les risques offre la possibilité aux entités d'adapter leurs mesures en fonction des situations de risques auxquelles elles sont confrontées et d'améliorer le rapport coûts bénéfices du système de LBC/FT mis en place au sein même de l'entité. (BNB, 2019)

Deuxièmement, une évaluation des risques associés à chaque client est également requise par la législation belge. Le but de cet instrument est de définir pour chaque client l'intensité des mesures de vigilance qui doivent être appliquées ou, le cas échéant, de refuser de nouer la relation d'affaire. (BNB, 2019)

Ces évaluations, globales et individuelles, ne sont pas des exercices uniques mais bien des processus permanents qui doivent être mis à jour chaque fois que se produisent « *un ou plusieurs événements susceptibles d'avoir une influence significative sur les risques* » (BNB, 2019).

À la fin de cette section, il est intéressant de s'attarder sur la notion de complémentarité présente entre chacun des échelons de cette pyramide. Nous avons abordé cette « chaîne de LBC/FT» en partant des organismes émetteurs des normes en matière de LBC/FT pour montrer l'influence de chaque niveau sur celui en-dessous. Toutefois, la présentation de cette pyramide pourrait également avoir lieu en sens inverse puisque, finalement, l'approche préventive de la LBC/FT débute avec l'implication des entités assujetties. Les évaluations globales des risques, effectuées par l'ensemble des entités assujetties d'un pays, fournissent des renseignements utiles aux acteurs nationaux et facilitent ainsi la réalisation de l'évaluation nationale des risques de BC/FT. En outre, ces évaluations nationales jouent à leur tour un rôle primordial pour le rapport de la Commission européenne et contribuent au travail des CRF et des législateurs internationaux, qui essaient constamment d'adapter les normes internationales aux nouvelles tendances du BC/FT.

5.3. La mise en place de l'approche fondée sur les risques en Belgique

Aujourd'hui, la RBA peut être considérée comme la pierre angulaire des mécanismes préventifs en matière de BC/FT. Comme expliqué précédemment, son application généralisée permet d'améliorer, à tous les niveaux, l'allocation des ressources et d'atteindre ainsi une efficacité aussi grande que possible de la prévention. L'objectif essentiel de la législation anti-blanchiment est de « *réduire dans toute la mesure du possible les risques AML au sein des institutions et* (de) *requérir d'elles une réaction appropriée lorsque ces risques se matérialisent, afin d'empêcher qu'ils se propagent au secteur financier et dans la société en général* ». Visant plus qu'un simple objectif de conformité de la part des institutions, la Loi du 18 septembre 2017 espère détecter et empêcher la réalisation d'opérations liées au

BC/FT. Cependant, cet objectif ne doit pas être interprété comme constituant une obligation de résultat, ce qui serait incompatible avec l'approche fondée sur les risques. (GATOT, 2019)

5.3.1. L'environnement de contrôle

Pour atteindre l'objectif fixé par la Loi, les institutions sont tenues de mettre en place un dispositif de gestion des risques en matière de LBC/FT efficace et proportionné à leur nature et à leur taille. À travers le modèle des trois lignes de défense proposé par l'Institut des Auditeurs Internes, nous allons analyser comment l'approche fondée sur les risques peut être implémentée dans l'organisation d'une institution.

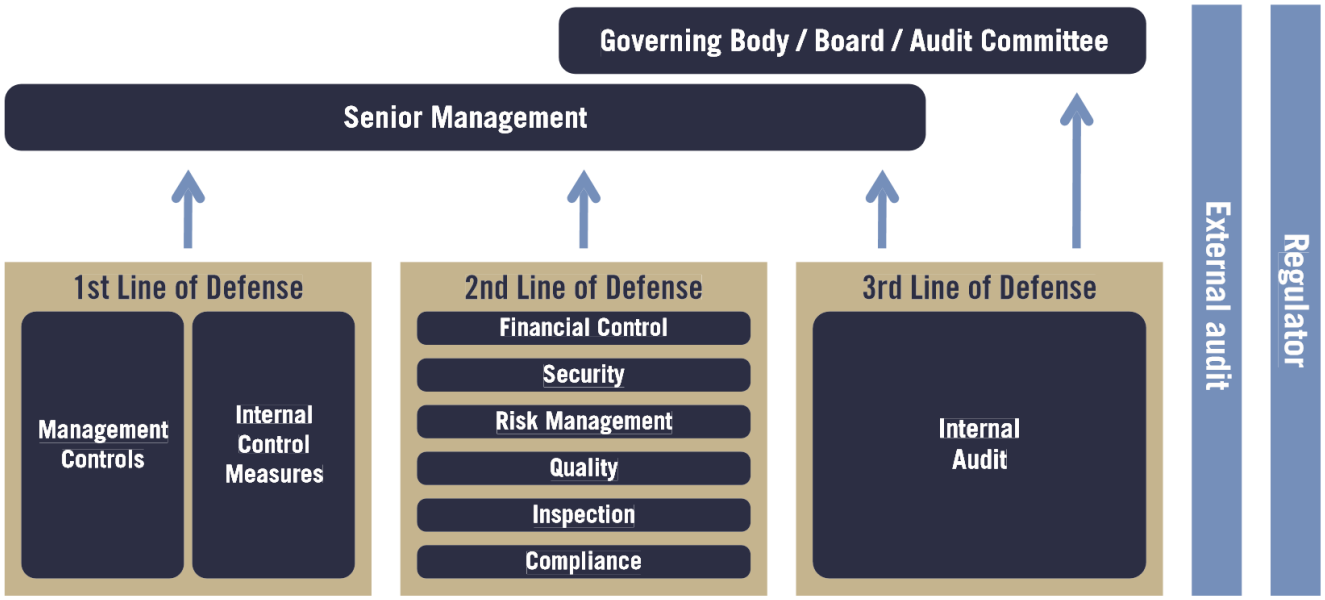


Figure 5.1 : Les trois lignes de défense d'une gestion et d'un contrôle efficaces des risques
Source : The Institute of Internal Auditors, 2013, p.2

Le Conseil d'Administration est l'organe de décision de la stratégie et des objectifs de l'institution. Dès lors, c'est à lui de déterminer la stratégie générale en matière de gestion des risques de BC/FT et de valider la politique en matière de LBC/FT de l'institution tout en restant informé sur les résultats du dispositif à l'aide de rapports en la matière. (BNB, 2019)

Le Comité de Direction met en œuvre la stratégie de LBC/FT définie par le Conseil d'Administration. En ce sens, il est notamment responsable de la structure de l'organisation, des procédures internes et des mécanismes de contrôle interne en matière LBC/FT afin de respecter les lois et la stratégie globale de l'institution. Il doit également évaluer l'efficacité de son système de gouvernance et assurer une communication efficace du *reporting* en interne mais aussi vis-à-vis des autorités externes de contrôle. (BNB, 2019)

Au niveau des managers responsables de la gestion des risques BC/FT, deux fonctions de gouvernance se démarquent particulièrement : le haut dirigeant responsable et *l'Anti-Money Laundering Compliance Officer*, plus communément désigné sous l'abréviation AMLCO.

Selon l'article 9 de la Loi, le haut dirigeant responsable doit être désigné « *parmi les membres de leur organe légal d'administration ou, le cas échéant, de leur direction effective*». Cette obligation a pour objectif principal de renforcer l'implication du plus haut niveau hiérarchique des institutions dans la gestion des risques de BC/FT. Le haut dirigeant responsable doit répondre à des conditions d'honorabilité et d'expertise en matière LBC/FT, vérifiées au préalable par un examen (*screening fit & proper)* réalisé par la BNB ou par la Banque Centrale Européenne. L'absence de conflit d'intérêts étant une condition sine qua non à la réalisation de sa mission, cette tâche ne peut être cumulée avec d'autres tâches génératrices de risques de BC/FT. (BNB, 2019)

L'AMLCO est la personne chargée de la mise en œuvre et du pilotage concret du dispositif LBC/FT. Ses fonctions relèvent notamment de l'analyse des opérations atypiques, de l'élaboration d'un programme annuel de *monitoring*, de la formation des membres du personnel et de la rédaction des rapports internes réalisés à cet effet. En fonction de la nature, de la taille et du profil de risques de l'institution, il peut travailler seul ou être la tête d'une « cellule *AML* ». En plus des conditions d'honorabilité et d'expertise auxquelles il doit également répondre, l'AMLCO doit disposer du niveau hiérarchique et de la disponibilité nécessaires à l'exercice effectif, indépendant et autonome de ses fonctions. (BNB, 2019)

La première ligne de défense repose sur les activités de contrôle et de surveillance quotidiennes effectuées par les collaborateurs. Cette première ligne assume le risque et se doit de gérer celui-ci en fonction des politiques et procédures mises en place par l'institution. Le management doit alors intervenir dans l'implémentation de contrôles efficaces et dans la formation et la sensibilisation de ces collaborateurs. (GATOT, 2019 ; ANDERSON et EUBANKS, 2015)

La deuxième ligne de défense regroupe les activités de contrôle opérées par des fonctions indépendantes telles que le département *Compliance* ou le département *AML*. Basée sur le monitoring effectué à la première ligne, elle opère des contrôles spécifiques en apportant l'expertise, les conseils et les supports nécessaires à l'analyse. Cette deuxième ligne assure la coordination de la gestion et de la surveillance des risques auxquels l'institution est exposée. (GATOT, 2019 ; ANDERSON et EUBANKS, 2015)

Finalement, la troisième ligne concerne les activités de contrôle périodique qui fournissent une assurance indépendante au management et à la direction de l'institution concernant l'efficacité de leur

politique de gestion des risques. Cet audit interne permet de s'assurer du bon déroulement des contrôles effectués aux deux lignes précédentes. (GATOT, 2019)

Des audits externes sont également effectués par les autorités de contrôle compétentes qui peuvent exercer soit un contrôle sur place soit un contrôle à distance sur base des documents fournis par les entités. Dans le cas des institutions financières, les documents principaux à fournir au moins une fois par an à la BNB sont le questionnaire périodique, le rapport d'activité de l'AMLCO et les documents concernant l'évaluation globale des risques dont nous parlerons dans la sous-section suivante. La BNB va, entre autres, vérifier si l'entité a bel et bien respecté le principe de proportionnalité dans ses décisions, procédures et mesures. Pour ce faire, elle tient compte de la nature, du statut et de la taille de l'institution mais également de la nature et de la complexité de ses opérations. (BNB, 2019)

En ce sens, les institutions doivent pouvoir prouver à ces autorités que leurs procédures, leurs mesures de contrôle ainsi que leurs politiques d'acceptation des clients sont documentées, mises à jour à chaque fois que cela est nécessaire et en adéquation avec les niveaux de risques établis. Pour faciliter les obligations des institutions et leur permettre d'établir correctement ces niveaux de risques, un nouvel instrument est apparu dans la Loi, l'évaluation globale des risques de BC/FT. (Loi du 18 septembre 2017, Art. 17)

5.3.2. L'évaluation globale

L'évaluation globale des risques, en anglais *business-wide risk assessment* [ci-après BWRA], est un instrument utilisé par les institutions financières qui leur permet d'identifier et gérer de manière appropriée les risques inhérents en matière BC/FT. Les articles 16 à 18 de la Loi du 18 septembre 2017 lui sont consacrés (Cf. Annexe 6, L'évaluation globale des risques dans la Loi *AML*). Pour réaliser cette évaluation, les institutions doivent mettre en œuvre trois grandes phases successives : l'identification, l'analyse et l'ajustement.

La première phase de l'évaluation globale des risques consiste en une identification et une compréhension approfondie des risques de BC/FT auxquels est exposée l'institution. Celle-ci doit identifier tous les risques qui la concernent et les classer en catégories et sous-catégories selon les caractéristiques de sa clientèle, les produits, services et opérations qu'elle offre, les pays ou zones géographiques avec qui elle traite et les canaux de distribution auxquels elle a recours. Une fois les risques inventoriés, il faut analyser l'exposition à ces risques. Pour ce faire, l'institution doit au moins prendre en considération la finalité des comptes ou des relations, le niveau d'actifs déposés par les clients ou le volume des opérations effectuées et la régularité ou la durée des relations d'affaires. À ces variables

doivent également s'ajouter les facteurs spécifiques, indicatifs d'un risque potentiellement plus ou moins élevé, définis dans les annexes de la Loi. Cette analyse engendre alors un score de risque inhérent propre à chaque catégorie qui prend également en compte la probabilité d'occurrence des risques. Le nombre de classes de risque dépend de l'approche adoptée par les organismes. Certains se sont alignés sur la règlementation en retenant uniquement trois classes de risques mais d'autres ont affiné leur approche en définissant des scores allant de limité à très élevé. (BNB, 2019 ; Loi du 18 septembre 2017, Art.16)

Vient ensuite la phase d'analyse du *gap*[28] qui fait l'inventaire des mesures de gestion des risques déjà établies par l'institution et évalue si ces mesures sont suffisantes pour gérer ou limiter les différents risques identifiés. En plus de tenir compte de ces mesures déjà mises en place, il est important de regarder la manière dont ces mesures sont effectivement appliquées et respectées dans la pratique au sein de l'institution pour évaluer si elles sont véritablement efficaces. (BNB, 2019)

Si, à l'issue de la phase d'analyse, les mesures existantes sont insuffisantes par rapport au seuil de tolérance maximale aux risques de l'institution, de nouvelles solutions de gestion des risques doivent être mises en place. C'est la phase d'ajustement, dernière phase de ce processus d'évaluation globale. Lorsque le risque résiduel, c'est-à-dire le risque résultant après les mesures existantes, est supérieur à ce seuil de tolérance, une réévaluation du système de contrôle interne et des solutions supplémentaires sont nécessaires pour amener ce risque résiduel en-dessous du seuil. L'institution peut mettre en œuvre certaines mesures réduisant l'impact ou la probabilité d'occurrence de ce risque, d'autres mesures permettant de partager ou transférer le risque au travers d'une assurance ou d'un contrat. Arrêter les activités à l'origine du risque est également une solution envisageable lorsqu'aucune mesure ne permet de réduire ce risque à un niveau acceptable. (GATOT, 2019) En outre, l'institution est tenue de définir un délai et de prévoir des moyens pour la mise en œuvre concrète de ces différentes solutions. Pour parvenir à un résultat efficace, elle doit tenir compte non seulement de l'ampleur, de la gravité et de l'incidence du risque non couvert mais aussi de l'ampleur et de la complexité des mesures d'ajustement à prendre. Ainsi, les mesures plus facilement applicables avec un impact important sur les risques deviendront une priorité. (BNB, 2019)

Par conséquent, le résultat de l'évaluation globale d'une institution détermine de façon adéquate et proportionnée les politiques de gouvernance, les procédures, les mesures de contrôle interne et l'allocation des ressources humaines et matérielles nécessaires que celle-ci doit mettre en place dans le cadre de la LBC/FT.

[28] Écart en anglais.

5.3.3. L'évaluation individuelle

En plus de l'évaluation globale des risques de BC/FT auxquels l'institution est exposée, la mise en œuvre de l'approche fondée sur les risques exige également une évaluation des risques associés à chaque relation d'affaires ou opération occasionnelle. Tout en tenant compte de l'évaluation globale, cette évaluation individuelle considère les particularités du client ou de l'opération occasionnelle. Elle analyse notamment les informations relatives à l'identité et aux caractéristiques du client, les informations relatives à l'objet et à la nature de la relation d'affaires et toutes autres informations recueillies dans le cadre des obligations de vigilance. (Loi du 18 septembre 2017, Art.19)

Il y a trois principales obligations de vigilance à l'égard de la clientèle et des opérations : l'obligation d'identification et de vérification de l'identité du client[29], l'obligation d'identification des caractéristiques du client et de l'objet et de la nature de la relation ou de l'opération occasionnelle et enfin, l'obligation d'exercer une vigilance continue à l'égard des relations d'affaires et des opérations. Ces obligations vont permettre à l'institution de recueillir un maximum d'informations qui vont alors être utilisées dans l'évaluation individuelle des risques. Une des méthodes d'évaluation consiste à attribuer un score à chacun des facteurs de risque et à combiner ceux-ci en suivant quelques recommandations établies par les Autorités Européennes de Surveillance[30] [ci-après AES] concernant la pondération de ces scores. L'évaluation individuelle permet à l'institution de classer chaque relation d'affaire ou opération occasionnelle dans les catégories de risques déterminées lors de l'évaluation globale et leur attribue ainsi un profil de risque de BC/FT : élevé, standard ou éventuellement faible. (BNB, 2019)

A l'issue de l'évaluation individuelle des risques, l'institution financière va alors déterminer quel est, pour chaque client ou opération occasionnelle, le niveau de vigilance – accrue, standard ou simplifiée – à appliquer aux opérations réalisées. En effet, les obligations de vigilance citées dans le paragraphe précédent sont également soumises à la RBA. En cas de risque de BC/FT faible, diverses mesures de vigilance simplifiée peuvent être mises en œuvre telles que l'exemption d'identification, la limitation du nombre de documents probants à fournir ou bien un *monitoring* allégé. À l'inverse, en cas de risque élevé, des mesures de vigilance renforcée doivent s'appliquer à l'égard de la clientèle comme par exemple la demande de données d'identification additionnelles, l'autorisation hiérarchique pour l'entrée en relation ou encore un *monitoring* transactionnel renforcé. La mise en place de la RBA au niveau des

[29] Et dans le cas échéant, l'identité de ses mandataires et de ses bénéficiaires effectifs

[30] Les trois Autorités européennes de surveillance sont l'*European Banking Authority* (EBA), l'*European Insurance and Occupational Pensions Authority* (EIOPA) et l'*European Securities and Markets Authority* (ESMA).

obligations de vigilance favorise une meilleure allocation des ressources au niveau de la surveillance des opérations bancaires. (GATOT, 2019)

Même si les procédures d'identification et de vérification qui ont lieu avant de nouer la relation d'affaire sont nécessaires, la procédure de suivi du risque tout au long de cette relation est tout aussi importante, sinon d'avantage. Ce suivi régulier est assuré par l'obligation de vigilance continue ; elle comprend l'examen attentif des opérations (avec d'éventuelles déclarations à la CTIF) et la mise à jour périodique des informations recueillies dans le cadre de l'évaluation individuelle. Si de nouvelles informations pertinentes conduisent à identifier des risques de BC/FT plus élevés ou plus faibles, alors l'institution reclassera le client dans une autre catégorie, un autre profil de risque pour gérer de façon optimale les nouveaux risques auxquels elle fait face. (GATOT, 2019)

DEUXIEME PARTIE : ANALYSE DE LA MISE EN ŒUVRE DE L'APPROCHE FONDÉE SUR LES RISQUES DANS LE SYSTÈME PRÉVENTIF BELGE

Chapitre 6 : La problématique et la méthodologie de l'étude

6.1. La problématique

Des éléments exposés au niveau de la première partie, nous ne pouvons que constater l'importance des mesures de prévention en matière de LBC/FT. Les législateurs ont estimé qu'une bonne compréhension des risques potentiels permettait de gérer de manière efficace la menace constante du blanchiment et du financement du terrorisme. Ils ont alors consacré l'approche fondée sur les risques et défini de nombreuses obligations et mesures devant être mises en œuvre, entre autres, par les acteurs privés.

Aujourd'hui, la loi du 18 septembre 2017 et les obligations qui en découlent ont normalement dû être appliquées par les entités assujetties. Il devient alors intéressant de se pencher sur la mise en œuvre effective des mesures de LBC/FT au sein de ces entités et plus particulièrement des institutions financières[31] sous le contrôle de la BNB, qui tiennent une place important dans le dispositif de LBC/FT en Belgique au vu du nombre d'opérations financières qu'elles traitent quotidiennement.

En ce sens, nous analyserons dans le chapitre 7 le cas particulier d'une entité assujettie à travers l'étude d'un établissement de crédit. L'objectif sera d'observer la manière dont cette banque a réagi face à la nouvelle législation, notamment dans la mise en œuvre du processus d'évaluation globale des risques, et ce qu'elle lui a apporté. Nous développerons ensuite les considérations de la BNB en tant qu'autorité de contrôle, ses premières conclusions concernant le BWRA et ses attentes envers les institutions financières. Enfin, le chapitre 8 exposera une partie des enjeux actuels de la LBC/FT en Belgique et apportera quelques pistes de solutions pour améliorer l'efficacité des dispositifs mis en place par les acteurs impliqués dans cette lutte.

[31] Le terme « institutions financières » dénomme de manière collective les entités suivantes : les établissements de crédit, les entreprises d'assurance, les établissements de paiement, les émetteurs de monnaie électronique, les organismes de liquidation, les dépositaires centraux de titres, les sociétés de cautionnement mutuel, les sociétés de bourse ainsi que l'ensemble des succursales de ce type d'entités situées en Belgique. (BNB, 2019)

6.2. La méthodologie

L'analyse consiste en une étude exploratoire, méthode qualitative, qui généralement « *a pour objectif de comprendre un phénomène selon la perspective des sujets et du contexte* » (DUFOUR, 2019). Ce type d'étude offre un processus de recherche plutôt informel et souple qui permet de travailler avec un échantillon restreint et non-représentatif (DESSART et STEILS, 2016). Parmi les méthodes de recherche possibles, nous nous concentrerons sur des analyses documentaires appuyées par un entretien réalisé avec un expert en matière de LBC/FT.

L'analyse se base premièrement sur certains articles récents, publiés à la suite de l'entrée en vigueur de la Loi du 18 septembre 2017, qui seront cités tout au long des chapitres suivants. Ils proposent généralement une première analyse des implications de cette loi, de son efficacité et mettent en lumière quelques critiques à son égard. À cette source documentaire vient s'ajouter les rapports annuels d'activités de la CTIF. Depuis le début de ses activités, la Cellule dégage à partir des dossiers transmis un certain nombre d'informations pertinentes telles que l'analyse des tendances en matière de BC/FT ainsi que les statistiques relatives aux dossiers transmis au Procureur du Roi. Plusieurs textes de loi et documents émis par la BNB, comme les circulaires ou certaines de ses recommandations, serviront également nos recherches.

En outre, nous avons réalisé l'étude du cas d'une entité assujettie soumise à la Loi en combinant l'analyse de documents mis à notre disposition et les informations récoltées au cours d'une rencontre avec un collaborateur de la société, expert en BWRA. Selon le Larousse, le terme d'expert est défini comme étant « *quelqu'un qui connaît très bien quelque chose, par la pratique* ». Etant responsable d'une grande partie du dispositif de LBC/FT mis en place dans une institution financière, en particulier du BWRA, notre intervenant peut dès lors être considéré comme un expert dans son domaine.

Pour cet entretien d'une heure trente, nous avons privilégié une approche non directive puisqu'elle favorise l'ouverture et la flexibilité dans la discussion. Parler des dispositifs de LBC/FT mis en œuvre par une institution financière est un sujet délicat et assez confidentiel, il était donc primordial d'installer un climat de confiance avec l'expert interrogé en privilégiant une « conversation naturelle » et en limitant les interventions de l'enquêteur pour obtenir des informations riches et pertinentes (DESSART et STEILS, 2016). Compte tenu du type d'entretien choisi, le suivi d'un guide d'entretien très structuré durant l'interview n'est pas nécessaire. Nous avons cependant élaboré au préalable un schéma d'entretien reprenant l'introduction de la problématique ainsi qu'une liste de questions liées aux thèmes à explorer avec l'expert (Cf. Annexe 5, Le plan de l'interview). Toutes les questions figurant sur

la liste n'ont pas été abordées telles quelles mais les grands thèmes auxquelles elles font référence ont été discutés.

Dans un souci déontologique, aucune des informations qui permettraient d'identifier l'institution financière ou l'expert interrogé ne sera divulguée afin d'assurer l'anonymat de l'entité assujettie analysée dans l'étude de cas ainsi que la confidentialité des informations sensibles qui auraient pu être transmises.

La plus grande limite de cette étude est relative à la taille de l'échantillon analysé. En effet, nous n'analyserons qu'une seule entité assujettie et, même si les établissements de crédit jouent un rôle prépondérant dans la LBC/FT, il est possible que ce cas ne soit pas représentatif de la situation des autres entités face à l'approche fondée sur les risques ou à l'évaluation globale. Dès lors, l'échantillon de données à notre disposition peut être qualifié de restrictif. Cela s'explique entre autres par le caractère confidentiel du sujet traité pour lequel les entités assujetties, souvent engagées dans des activités commerciales, ne dévoilent leur stratégie de gestion des risques ni à la concurrence, ni à leurs clients et futurs clients potentiels.

Chapitre 7 : La mise en œuvre de l'évaluation globale des risques depuis l'entrée en vigueur de la Loi du 18 septembre 2017

7.1. L'étude du cas d'une entité assujettie

Selon la Loi bancaire[32], l'entité assujettie dont nous aller discuter tout au long de cette analyse peut être définie comme un établissement de crédit[33] de taille moyenne. Dès lors, elle fait partie des entités assujetties soumises aux obligations de la Loi du 18 septembre 2017 (Loi du 18 septembre 2017, Art.5). C'est donc sur base de cette loi que le dispositif de LBC/FT de cette institution financière est mis en œuvre.

7.1.1. Évaluation globale

Bien que l'évaluation globale des risques soit une nouvelle exigence de la Loi, sa base juridique, les articles 16 à 18 (Cf. Annexe 6, L'évaluation globale des risques dans la Loi AML), laisse aux entités une grande liberté d'interprétation pour effectuer l'évaluation. Cette liberté est conservée dans les recommandations de la BNB, qui ne donne finalement que très peu des consignes concernant le BWRA, ce qui explique aussi la difficulté de l'exercice. En effet, notre expert nous a expliqué que la première réalisation de l'évaluation globale n'a pas été des plus simples. Que ce soit dans les médias ou les groupes de travail organisés chez Febelfin[34], il n'y avait pas de discussions sur le sujet en tant que tel parce que, finalement, tout le monde a réagi à sa manière et de son côté. Après quelques réunions organisées en interne avec le haut dirigeant responsable et l'AMLCO, l'établissement de crédit s'est lancé dans l'exercice.

<u>L'identification</u>

Après un premier passage au crible de tous les textes législatifs européens et belges, la personne en charge de l'évaluation a appliqué l'article 16 en faisant tout d'abord l'inventaire des différents risques. L'inventaire de cet établissement de crédit est divisé en 5 grandes catégories de risques, elles-mêmes subdivisées en sous-catégories[35]. La première regroupe les risques liés aux clients où nous retrouvons

---

[32] Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourses.

[33] « *[…] sont définies comme établissement de crédit, les entreprises belges ou étrangères dont l'activité consiste à recevoir du public de départ d'argent ou d'autres fonds remboursables et à octroyer des crédits pour leur propre compte.* » (Loi du 25 avril 2014, Art.1, §3)

[34] Fédération Belge du secteur Financier

[35] Les exemples de catégories et sous-catégories suivants sont des listes non-exhaustives afin de protéger l'anonymat de l'établissement de crédit.

les personnes physiques et des personnes morales réparties en plusieurs sous-catégories comme ASBL, résident belge, résident dans un pays à risque, personne politiquement exposée, trusts, etc. Une seconde catégorie contient l'ensemble des produits et services offerts tels que les crédits hypothécaires, les différentes sortes de comptes ou encore les assurances. Les canaux de distribution utilisés par l'établissement sont également listés dans une troisième catégorie où l'on retrouve par exemple les courtiers, le service clientèle, le pc-Banking et le mobile-Banking. La quatrième catégorie fait l'inventaire de tous les types d'opérations de paiement autorisées par la banque telles que les dépôts en espèces, les paiements nationaux ou transnationaux, etc. Enfin, la dernière catégorie reprend les risques généraux où les sous-catégories sont, par exemple, l'absence d'identification/vérification des clients, les ressources *Compliance* insuffisantes ou encore le non-respect des dispositions contraignantes en matière de sanctions financières et d'embargos et d'autres mesures. Il va sans dire qu'un tel travail demande un niveau de collaboration important de la part de tous les départements de la banque puisqu'ils sont tous impliqués dans cet exercice global.

Une fois cet inventaire terminé, il faut quantifier chacune des sous-catégories identifiées en déterminant leur probabilité d'occurrence. Cette statistique, calculée sur base d'une formule propre à cette institution financière, dépend du nombre de clients et de transactions impactées par chaque sous-catégorie de risque. Sur base de cette donnée et du niveau de risque réglementaire défini par les autorités[36] pour chacune des sous-catégories, le responsable BWRA détermine le niveau d'exposition au risque résultant suivant ce graphe :

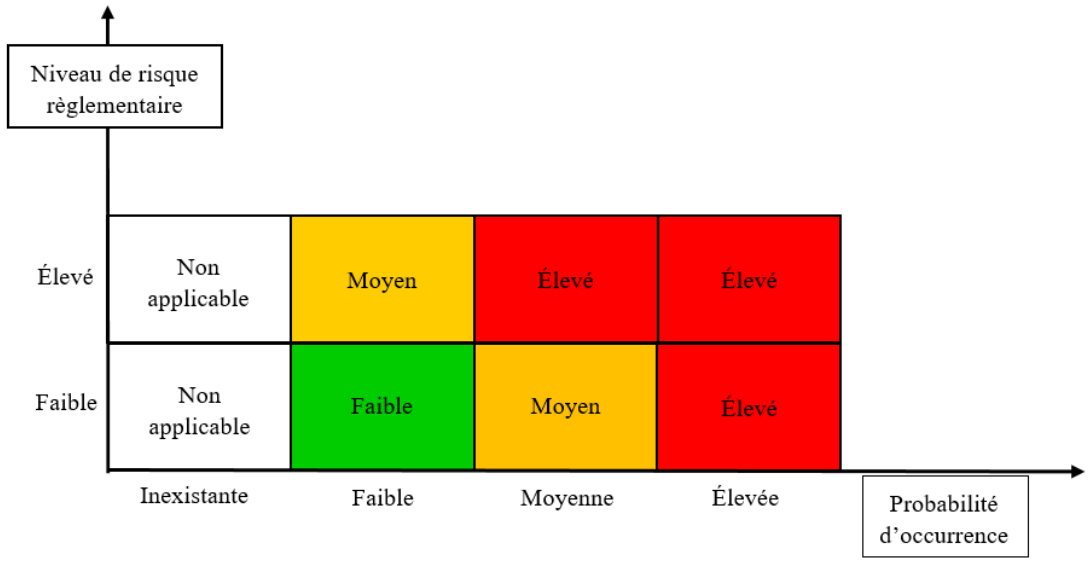


Figure 7.1 : Mesure du niveau d'exposition au risque

[36] Les documents pris en compte par cet établissement de crédit sont la Loi du 18 septembre 2017, l'orientation sur les facteurs de risque de l'ESA et les conclusions de la Commission européenne au titre de l'art. 6 de la directive 2015/849 de l'UE relative à la lutte contre le blanchiment de capitaux.

L'analyse

L'étape suivante est l'évaluation du risque résiduel pour chacune des sous-catégories de risques identifiés et quantifiés. Pour ce faire, l'établissement de crédit effectue en premier lieu un inventaire des différentes mesures déjà existantes pour réduire les risques de BC/FT et évalue ensuite leur niveau d'adéquation selon deux critères : la conformité et l'implémentation effective. Un « test de conception » vérifie la conformité des mesures en analysant leurs lacunes par rapport aux exigences légales, aux recommandations de la BNB et aux conclusions des différents rapports de LBC/FT effectués au sein même de l'établissement. L'implémentation effective est, quant à elle, vérifiée à l'aide des résultats des tests du *Compliance Monitoring Program* et des informations, rapports ou encore recommandations internes en matière de LBC/FT et de *Compliance.* Sur base de ces critères de conformité et d'effectivité, la banque détermine alors trois niveaux d'adéquation – parfaitement adéquat, largement adéquat et partiellement adéquat – calculés comme suit :

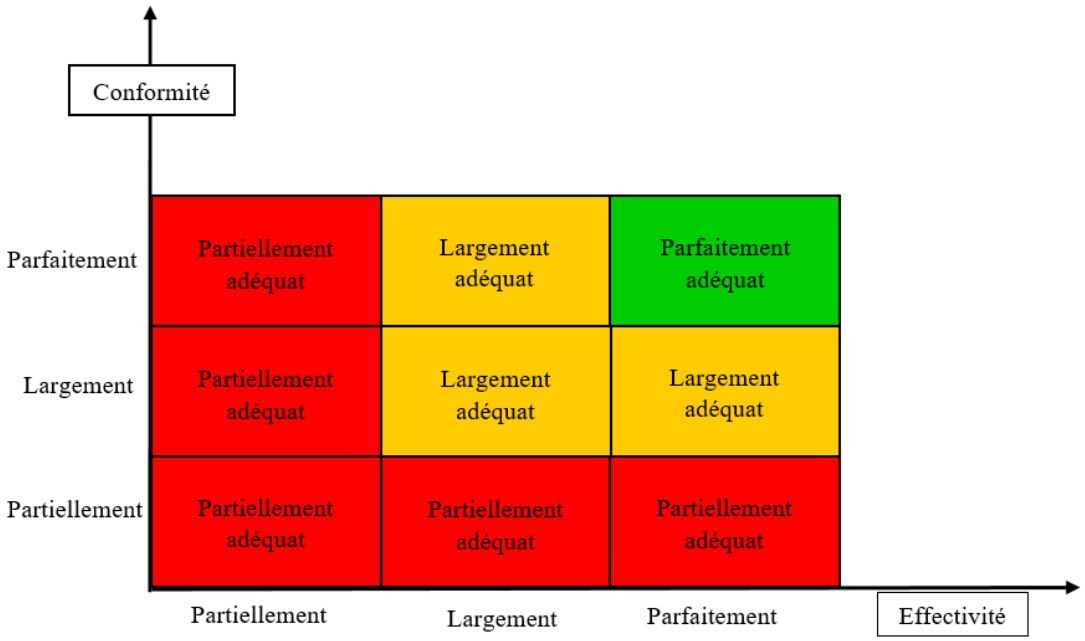


Figure 7.2 : Mesure du niveau d'adéquation des mesures existantes au sein de l'établissement de crédit

Lorsqu'une mesure est catégorisée comme « largement adéquate », cela signifie qu'elle présente le niveau d'adéquation minimum que la banque est prête à accepter. En dessous de ce niveau, des mesures d'atténuation supplémentaires devraient être prises.

L'ajustement

La dernière étape de l'évaluation globale des risques définit et met en œuvre les mesures supplémentaires lorsque celles-ci sont nécessaires, c'est-à-dire lorsque les mesures existantes sont

considérées comme partiellement adéquates et largement adéquates. L'établissement de crédit avait déjà implémenté un grand nombre de mesures d'atténuation des risques et en a encore ajoutées une vingtaine en 2019, lors de son dernier exercice d'évaluation globale. Parmi celles-ci, on retrouve bien entendu les déclarations des opérations suspectes à la CTIF, les mesures d'identification et de vérification de l'identité des clients, mandataires et bénéficiaires effectifs avant l'entrée en relation, les processus de vérifications périodiques pour les clients à haut risques mais également les formations des membres du personnel, les procédures *AML* contenant les instructions relatives à l'exécution des tâches opérationnelles de LBC/FT ou encore les outils de monitoring et de screening qui permettent par exemple de générer des alertes automatiques en fonction des listes Dow Jones[37]. Lorsque l'établissement de crédit a défini les nouvelles mesures, il détermine également leur calendrier de mise en œuvre et leur impact informatique.

L'apport du BWRA

Chaque année, l'établissement de crédit rend trois grands exercices à la BNB : le rapport d'activité de l'AMLCO, le questionnaire périodique et enfin le BWRA. Pour maintenir un certain niveau de cohérence entre ces trois outils, ils exploitent les mêmes données mais de façon différente. Alors que l'AMLCO fait un rapport détaillé sur les activités de LBC/FT de l'établissement, le questionnaire périodique requiert principalement un grand nombre de données chiffrées[38]. Le BWRA propose une autre méthode de travail, utilisant certes les mêmes données, mais offrant une vue d'ensemble sur l'exposition aux risques de BC/FT de l'établissement. Cette évaluation met également en lumière certains éléments que la banque aurait « perdus de vue ». Le responsable BWRA nous explique :

> «
> *Imaginons, par exemple, le cas de clients "personnes morales" qui exerceraient des activités à risque. Si l'année dernière ils étaient 20 mais que les chiffres au 31 décembre 2019 s'élèvent à 100, cela va susciter des interrogations. Je vais, dans un premier temps, le communiquer dans le questionnaire périodique en notant qu'au 31 décembre 2019, ils sont 100. Ensuite, dans mon évaluation globale, je vais analyser les raisons et essayer de chercher plus loin pour déterminer pourquoi nous avons eu une augmentation de clientèle dans ce secteur à risque. Est-ce que l'on a un outil qui serait plus sensible à les détecter par rapport au passé ou est-ce que l'on vient tout simplement de mettre en production un compte qui va attirer plus de personnes morales ? Si c'est quelque chose de risqué et que la banque n'est pas d'accord d'accepter ce risque, alors je vais*

[37] Base de données commerciale reprenant par exemple des listes de PPE au niveau international

[38] Ces questionnaires périodiques vierges sont disponibles sur le site de la BNB.

veiller à réduire ce risque. Par exemple, la politique d'acceptation de la clientèle peut être adaptée et nous pouvons décider que tel ou tel secteur de risque va être considéré à très haut risque à partir d'aujourd'hui et ainsi adapter le monitoring dans nos outils pour qu'ils deviennent beaucoup plus sensibles dans les transactions de cette clientèle et généreront plus d'alertes pour les personnes morales. »

Finalement, le BWRA va lister l'ensemble des risques BC/FT présentés par tous leurs clients, produits, services, opérations, canaux de distribution, va les quantifier et faire en même temps l'inventaire complet des mesures déjà mises en place et de leur efficacité ; le tout présenté sur un seul et unique support (Cf. Annexe 7, Un exemple de support de BWRA). Grâce à cette vue globale, l'établissement de crédit discerne aisément et rapidement les faiblesses de son dispositif de LBC/FT et peut ainsi y remédier de la façon la plus optimale possible.

7.1.2. Exercice perpétuel

Même si le BWRA se fait de façon périodique, évaluer les risques de BC/FT liés aux clients et aux opérations est un exercice continu. En effet, les outils de *screening* et de *monitoring* ne cessent jamais de tourner et génèrent automatiquement, en fonction des paramètres déterminés par la banque, des alertes sur les transactions. Ensuite, ce sont des collaborateurs spécialisés qui vont analyser ces alertes et déterminer la véracité des données générées par le système.

Il est important de noter que ces alertes n'ont pas uniquement lieu après l'entrée en relation avec un client. Ces outils de vérification sont également présents lorsqu'un client potentiel va entrer en contact avec la banque. La politique d'acceptation de la clientèle a des critères bien déterminés, notamment en matière de LBC/FT, et intégrés dans les outils du service clientèle. Ainsi, lorsqu'un client qui présente un profil à risque désire ouvrir un compte ou effectuer une quelconque opération, il fera d'abord l'objet d'une évaluation individuelle réalisée par les spécialistes *AML*. Sur base de celle-ci, la banque décidera si elle désire rentrer en relation avec la personne.

Cette évaluation perpétuelle des risques de BC/FT s'applique non seulement aux clients potentiels mais aussi à la clientèle acquise avant l'entrée en vigueur de la Loi. Un exemple probant donné par notre expert durant l'interview est celui des PPE. Lorsqu'une une personne physique occupe ou a occupé une fonction publique importante, la législation demande aux entités assujetties de faire preuve de mesure de vigilance élevée à son égard ou celui de ses proches (Loi du 18 septembre 2017, Art.34). Pour respecter cette obligation, l'outil de *monitoring* et de *screening* de la banque croise continuellement la base de données de la clientèle avec les informations des listes nationales, européennes et internationales qui reprennent l'ensemble des PPE ainsi que les membres de leur famille. Une fois qu'une

alerte est générée par l'outil, celle-ci est traitée et vérifiée « manuellement » en vue d'adapter le profil de risque de BC/FT du client si nécessaire.

De plus, l'établissement de crédit doit également s'adapter en fonction des modifications qui ont lieu au niveau de la législation – nationale ou européenne – et des recommandations de la BNB, mises à jour de manière assez régulière. Ça a été le cas par exemple avec le *crowdfunding*. Au départ, l'établissement de crédit pensait que ce nouveau mode de financement ne le concernerait pas et puis finalement, le législateur européen a fini par intervenir avec un règlement[39] qui a été rendu applicable directement, sans qu'il n'y ait aucune loi de transposition. Il devient alors très important pour la banque de se tenir informée de ces actualisations pour vérifier, dans un premier lieu, si elle est concernée par l'objet de la modification et, dans le cas échéant, pour l'implémenter le plus rapidement possible en cas de contrôle de la part des autorités compétentes.

7.1.3. Responsabilité de l'établissement de crédit

Pour atteindre son objectif de conformité en matière de LBC/FT, l'établissement de crédit est tenu de satisfaire les obligations définies par la Loi et de remettre une série de rapports annuels, dont le BWRA, à la BNB. Une fois le BWRA déposé, la BNB examine attentivement celui-ci et pose souvent quelques questions additionnelles assez ciblées qui concernent certaines mesures implémentées ou en devenir. Toutefois, la BNB n'effectue pas de retour précis vers l'entité concernant son évaluation sauf en cas de problème majeur. Certes, un dialogue est possible entre la BNB et les entités assujetties, mais, selon notre expert, ce dialogue doit venir sur l'initiative de l'établissement de crédit. Il explique que, lorsque la mise en œuvre de certaines mesures ne se déroule pas comme prévue en raison de telle ou telle situation, la banque doit prendre l'initiative d'aller vers la BNB pour les prévenir dès le début que l'échéance initiale planifiée dans le BWRA ne sera pas respectée. L'établissement de crédit se doit d'être honnête envers la Banque Nationale, non seulement parce qu'elle offre une possibilité de dialogue mais surtout parce qu'en cas de contrôle *on-site* des services d'inspection de la BNB, des mesures correctives ou des sanctions administratives peuvent être prises à l'égard de l'établissement de crédit, dégradant alors sa réputation.

L'établissement de crédit est également responsable des déclarations de soupçon qu'il transmet ou non à la CTIF. Lorsqu'une transaction parait suspecte, la banque réalise une sorte d'enquête sur le client concerné et puis estime si effectivement, cette transaction fait l'objet d'un soupçon. L'expert interrogé nous décrit ce procédé de recherche comme suit :

[39] Acte législatif contraignant devant être mis en œuvre dans son intégralité dans toute l'Union européenne (EUROPA ,2019)

« *Avant d'envoyer, avant de faire la déclaration à la CTIF, il faudra documenter ça. Il faudra faire un dossier sur le client, sur ce qu'il avait dans son historique, remonter dans son passé. Est-ce qu'il avait déjà fait ce genre de transactions ? Est-ce qu'on l'avait déjà dénoncé ? Est-ce qu'on avait reçu des demandes d'informations complémentaires de la part du parquet ou de la part de la CTIF ? On regarde un peu tout ça dans son dossier, dans son historique de transactions et puis on va chercher s'il est connu comme étant quelqu'un actif dans les secteurs à risques. Ça c'est sur Internet. Donc, on fait vraiment une enquête préliminaire et puis sur base de cette enquête, on prend une décision si, moi, en tant qu'employé du département Compliance, je peux me permettre de prendre l'initiative de le dénoncer.* »

Ce témoignage met en exergue l'importance du « premier filtre » opéré par les acteurs privés des entités assujetties. En déterminant, après enquête, quelles alertes générées par l'outil de *monitoring* doivent être signalées à la CTIF, chaque collaborateur endosse une certaine responsabilité envers le dispositif de LBC/FT.

7.1.4. Ressources engagées

Les législateurs belges et européens sont beaucoup plus sensibles au BC/FT qu'auparavant et deviennent donc de plus en plus sévères. Pour faire face au nombre croissant d'obligations auxquelles il est tenu, l'établissement de crédit étudié investit dans de nouvelles ressources technologiques et humaines.

Pour mettre en place un dispositif de LBC/FT efficient, l'ensemble des actions et transactions de la banque doit être continuellement vérifié de façon à détecter les opérations suspectes. Pour ce faire, l'établissement de crédit a investi dans un outil de *monitoring* et de *screening* générant des alertes en fonction des paramètres de sensibilités définis au préalable par l'établissement. Même s'il est créé par une entreprise extérieure spécialisée, l'outil peut se « personnaliser » pour faire varier la sensibilité des alertes selon les critères d'acceptation des clients et les indicateurs propres à l'établissement ou encore selon différents scénarios préétablis. Toutefois, un programme plus sophistiqué représente un plus grand investissement, sans compter l'achat périodique de nouvelles licences ou les actualisations futures. Comme le souligne notre expert, « *c'est là qu'on voit peut-être la différence au niveau du budget d'une banque par rapport à une autre, qui peut se permettre un programme plus développé* ». Une fois que les alertes sont générées, une équipe spécialisée au niveau opérationnel prend le relais et traite alors manuellement toutes ces informations.

Même si l'évolution technologique constante assiste les équipes *AML* dans la détection des opérations suspectes, des manipulations de la part d'une personne physique sont nécessaires pour traiter ces alertes, faire une vérification complète et chercher la véracité de données générées par le système. D'autres obligations influencent également le travail des collaborateurs *AML* comme la formation des nouveaux entrants mais aussi celle de leurs collègues travaillant dans d'autres départements de l'établissement. Afin d'assumer l'augmentation de sa charge de travail, l'équipe *AML* de la banque, qui était au départ assez limitée, a plus que doublé ces dernières années. Selon notre expert, l'établissement étudié n'est pas une exception. Aujourd'hui, toutes les institutions financières recherchent des conseillers dans la LBC/FT. En effet, lorsque l'on recherche une offre d'emploi en tant qu'*AML Compliance officer*, 23 propositions apparaissent sur Indeed et 34 sur LinkedIn, uniquement en Belgique…

Au vu des éléments exposés supra, nous pouvons conclure qu'en termes de coûts et d'investissements, l'impact de la Loi sur l'établissement de crédit étudié est assez considérable.

7.1.5. Apports de la Loi

Une des plus-values apportées par la loi de 2017 est la clarification des obligations de l'établissement de crédit. En effet, sa nouvelle structure rassemble dans un livre spécifique (Livre II) l'ensemble des obligations imposées aux entités permettant ainsi à l'établissement d'améliorer son dispositif BC/FT tout entier.

Autre nouveauté de cette nouvelle législation, le BWRA a permis à la banque d'avoir une vue d'ensemble sur les risques de BC/FT auxquels elle était exposée, d'adopter certaines mesures qui n'étaient pas encore mises en place, de perfectionner les formations de LBC/FT données aux collaborateurs ou encore d'améliorer leurs canaux de communication pour mieux faire circuler les informations à travers la société. Les responsables *AML* ont pris conscience qu'adopter une procédure n'était pas suffisant, il fallait aussi l'expliquer clairement aux personnes en contact avec la clientèle à l'aide d'exemples concrets, de séances de formations plus ciblées et d'une communication interdépartementale plus poussée. L'obligation d'actualisation de cette évaluation globale aide également la banque à maintenir son dispositif de LBC/FT à jour et lutter ainsi le plus efficacement possible contre ces criminalités.

L'approche fondée sur les risques, pierre angulaire du mécanisme actuel de LBC/FT consacrée par cette Loi, a modifié l'analyse des opérations suspectes. Autrefois, la Loi de 1993 défendait une approche basée sur les règles selon lesquelles la banque devait, par exemple, déclarer les transactions qui dépassaient un certain montant. La RBA met fin à ce procédé puisqu'aujourd'hui le montant de

l'opération importe peu. En effet, à partir du moment où l'on suspecte un risque de BC/FT et que cela ne correspond pas au profil connu du client de la banque, alors il sera déclaré à la CTIF.

Notons également que la Loi anti-blanchiment indique clairement que le dispositif LBC/FT doit être mis en place en suivant le principe de proportionnalité, selon lequel chaque entité alloue ses ressources humaines et financières au prorata de la taille de l'entité et de la nature de ses activités. L'établissement de crédit étudié étant de taille moyenne, ce principe se reflète, entre autres, dans la rédaction des procédures et des politiques de LBC/FT. Il est inutile de créer une procédure d'acceptation de la clientèle de 100 pages lorsque, premièrement, celle-ci peut être rédigée en 10 pages et que, deuxièmement, il n'y a pas assez de ressources humaines et informatiques pour assurer sa mise en place au sein de la banque.

7.2. Les observations au niveau national

Dans le cadre de la première mise en œuvre du processus de BWRA suivant l'entrée en vigueur de la Loi, les institutions étaient tenues de transmettre à la BNB une première version de leur évaluation globale à travers deux documents : un tableau récapitulatif donnant un aperçu général de la BWRA (Cf. Annexe 7, Un exemple de support de BWRA) et un document répondant à une série de questions ponctuelles à propos du processus de BWRA opéré (Cf. Annexe 8, Le questionnaire du BWRA). Cette première version était à rendre pour le 1er avril 2018 et la version définitive pour le 15 juillet 2018 au plus tard. Cette évaluation étant un exercice permanent, les institutions sont responsables de son actualisation et donc de la mise à jour des documents précités (BNB, 2019).

L'établissement de crédit étudié dans ce travail peut être considéré comme un « bon élève » en matière d'évaluation globale puisqu'il a non seulement déjà effectué deux exercices d'évaluation – le premier en 2018 et le deuxième en 2019 – mais aussi parce que, globalement, il n'a pas reçu de retours négatifs de la part de la BNB sur ceux-ci. Toutefois, ce n'est pas le cas de toutes les institutions supervisées par la Banque.

Après avoir reçu les exercices d'évaluation globale des entités sous sa supervision, la BNB les a analysés pour ensuite présenter ses premières observations sur la mise en place du processus lors de sessions de formations ou de réunions avec les hauts dirigeants responsables. En novembre 2019 lors d'une session d'information *AML*, Benoît Bienfait, conseiller à la BNB, a présenté les réflexions de la BNB basées sur les premières évaluations globales des risques des institutions. Les quatre paragraphes suivants résument ces observations. (BNB & CTIF, 2019)

En règle générale, les résultats obtenus après l'examen horizontal de ces évaluations sont assez mitigés. La Banque retrouve un certain nombre de très bons exemples qui, en règle générale, sont soit des groupes financiers – institutions financières déjà aguerries à ce type d'analyses des risques – soit des institutions financières « *stand alone* » et/ou de taille plus modeste – processus moins lourd par application du principe de proportionnalité. Par contre, elle a aussi dénombré un certain nombre de (très) mauvais exemples. Plusieurs institutions n'ont pas compris ni la finalité, ni l'importance de la BWRA ; elles ont réalisé leurs évaluations dans un simple objectif de conformité règlementaire en appliquant une approche purement formelle du processus. Malheureusement, lorsque ces institutions n'analysent pas en profondeur leurs lacunes existantes, la qualité des plans d'action mis en place devient également très variable et les mesures sont parfois peu concrètes ou non cohérentes avec les faiblesses identifiées (ex. une formation supplémentaire ne peut être une solution à tout).

La BNB qualifie de « perfectibles » les résultats obtenus jusqu'à présent dans la mise en place du processus de BWRA. Selon elle, il est nécessaire d'adopter des mesures supplémentaires en vue d'une amélioration du niveau des évaluations globales effectuées par les entités assujetties sous sa supervision.

Premièrement, la Banque s'intéresse à la mise en place de la procédure d'évaluation globale. Elle rappelle que celle-ci doit couvrir toutes les étapes logiques du BWRA, comme expliqué dans ses recommandations, et surtout qu'elle doit être approuvée par la Direction effective, gage de qualité et de professionnalisme. Elle met également l'accent sur la responsabilité du haut dirigeant et de l'AMLCO qui sont responsables de l'implication de leurs collaborateurs en contact direct avec les clients et les opérations, de l'approbation par la Direction effective du BWRA et des mesures mises en place qui en découlent. La Banque précise aussi que la synthèse communiquée à la BNB dans le cadre du *reporting* des institutions doit consister en un aperçu général du BWRA présenté sous une forme synthétique et simplifiée et donc, différer de la BWRA. En outre, certaines institutions présentent encore des difficultés pour discerner l'évaluation globale des risques – qui concerne les politiques et procédures de LBC/FT – et l'évaluation individuelle des risques – qui concerne l'entrée en relation d'affaires et le niveau des mesures de vigilance à appliquer.

Deuxièmement, la BNB analyse de façon isolée chacune des étapes du processus de BWRA. Le critère d'exhaustivité à appliquer lors de l'identification des risques est généralement bien respecté par les institutions. Pour l'analyse des risques, la Banque recommande aux institutions de se référer aux Orientations des AES sur les facteurs de risques pour leur garantir l'utilisation de facteurs de mesure des risques de BC/FT pertinents. Elle rappelle également la différence entre l'intensité, c'est-à-dire l'impact du risque, et l'exposition au risque, c'est-à-dire la probabilité d'occurrence du risque, ainsi que l'importance de différencier des classes de risques suffisamment homogènes. Pour ce qui est de la

gestion et de la réduction des risques, la BNB remarque que les plans d'actions prévus par les entités sont souvent très ambitieux tant dans la portée des mesures que dans leurs échéances de mise en place. Par ailleurs, elle attend de l'analyse des *gaps* un réel examen critique du dispositif LBC/FT qui peut alors s'inscrire dans une philosophie progressiste et non consister en une sorte de justification de « l'immobilisme des institutions financières ».

In fine, la BNB constate une grande disparité quant au degré de pertinence des évaluations globales, des analyses des gaps et des plans d'actions réalisés par les différentes institutions financières. Les différents points énumérés supra donnent un aperçu des faiblesses relevées dans les BWRA déjà réalisées par les institutions et ciblent ainsi les points à améliorer dans les exercices suivants. La Banque attend des institutions un réexamen de leur évaluation globale pour non seulement vérifier qu'elles rencontrent bien les standards de pertinence et de qualité attendus mais aussi pour que les institutions procèdent à une actualisation de leur évaluation.

Chapitre 8 : Les enjeux actuels

8.1. Les obligations imposées au secteur privé

Même si la lutte contre le blanchiment et le financement du terrorisme est avant tout la responsabilité des autorités, aujourd'hui sa mise en œuvre effective repose principalement sur les acteurs privés, dont les établissements de crédit – à l'origine de 74% des déclarations transmises au Parquet par la CTIF en 2018 (CTIF, 2018, p.46). En imposant aux professionnels assujettis le développement de politiques et de procédures qui les obligent à connaître leurs clients et à surveiller leurs opérations, les législateurs ont cependant fait naître une dualité dans les relations d'affaires de ces professionnels. En effet, une grande partie des entités assujetties concernées par les obligations de la Loi *AML* sont des commerçants : elles doivent donc inscrire leur action à la fois dans le cadre réglementaire de la LBC/FT et dans le cadre commercial de leurs activités. (TAUZIN, 2014, pp. 37-38)

Respecter les obligations de vigilance à l'égard de la clientèle relève parfois du défi pour les institutions et peut mettre en péril certaines relations d'affaires. Pour satisfaire à l'obligation de vérification des caractéristiques du client et de l'objet et de la nature de la relation, les institutions financières ont commencé à poser des questions assez précises à leurs clients. Comme l'explique BERDEN (2014, p.104), ces inquisitions n'ont pas toujours été bien accueillies ni par le personnel ni par la clientèle :

> « *Le message n'a pas été simple à faire passer dans les rangs commerciaux. En effet, le personnel des banques s'est très vite senti mal à l'aise vis-à-vis des clients : non seulement il devait leur demander de produire leur carte d'identité, mais voilà qu'il devait aussi les inviter à décrire leurs activités, donner, le cas échéant, les coordonnées de leur employeur et même confesser d'où provenait leur bas de laine … Sans compter qu'il fallait leur demander d'expliquer la nature et, si possible, le montant approximatif des opérations qu'ils envisageaient de faire auprès de la banque.* »

Si, aujourd'hui, les banques et leurs employés ont bien pris conscience de l'importance du dispositif de LBC/FT, l'expert interrogé confirme néanmoins que les réticences de certains clients sont toujours présentes.

Par exemple, lorsque le département *AML* manque d'informations sur certaines opérations atypiques, il peut passer par le service clientèle de l'établissement de crédit qui entre alors en contact avec les clients concernés pour leur poser quelques questions sur leurs opérations. Dans un certain nombre de cas, ces appels se soldent malheureusement par des réticences assez agressives, des menaces

de clôture des comptes ou encore une absence de réponse aux questions posées. Cette tâche est délicate car les commerciaux doivent, d'une part, recueillir des renseignements suffisamment précis pour éclairer l'avis du responsable *AML* chargé d'établir si l'opération est justifiée ou suspecte, et, d'autre part, ils ne peuvent pas laisser entendre au client qu'il fait ou pourrait faire l'objet d'une enquête pour soupçon de blanchiment ou de financement du terrorisme (BERDEN, 2014, p.111).

Un autre exemple d'actualité est celui des ouvertures de relations en ligne, réelle opportunité pour les établissements financiers d'attirer une nouvelle clientèle, de suivre la tendance du numérique qui est en en pleine expansion et d'étendre ainsi leur activité avec un nouveau canal de distribution. Mais comment les banques peuvent-elles concilier une procédure d'ouverture de compte en ligne avec l'ensemble de leurs obligations en matière d'identification ? Il est possible d'instaurer un questionnaire en ligne à remplir avant l'entrée en relation qui, dès lors, joue le rôle du contrôle de première ligne. Les banques doivent cependant réussir à créer un questionnaire assez complet pour dresser le profil de risques du futur client mais assez court pour satisfaire la promesse de rapidité du compte en ligne et empêcher ainsi la fuite de celui-ci chez un concurrent. À l'heure actuelle, les banques situées en Belgique ont généralement limité l'ouverture des relations en ligne à des personnes physiques, dont les vérifications sont plus aisées grâce aux cartes d'identité électroniques. Toutefois, l'ouverture de ces comptes pour les personnes morales reste un sujet de préoccupation pour le secteur financier.

Pour mettre en œuvre leurs obligations en matière de LBC/FT, certaines entités assujetties ont considérablement investi, tant humainement que matériellement, dans la conformité en matière de LBC/FT. Il est évident que le secteur financier occupe une place prépondérante parmi ces professions assujetties parce que non seulement il procède à un contrôle à la porte d'entrée de l'économie officielle, mais aussi parce qu'il est très vulnérable face au risque de réputation pouvant découler de l'utilisation abusive de ses systèmes (VERHAGE, 2014, p.119). Suivant le principe de proportionnalité prôné par la Loi, les institutions financières ont alors engagé de nouvelles ressources dans la LBC/FT. Tout comme l'établissement de crédit étudié, elles ont généralement amélioré les formations de leurs collaborateurs, agrandi leur équipe *AML* et investi dans des programmes de *screening* et de *monitoring* détectant les opérations atypiques.

Même si ces investissements dans les dispositifs de LBC/FT peuvent être aujourd'hui considérés comme des dépenses courantes pour les institutions, leurs coûts ne doivent pas être sous-estimés. Actuellement, le secteur de la conformité – qui couvre tous les services, instruments, sources d'informations susceptibles d'être utilisés par les entités dans la LBC/FT – est en pleine expansion. Les

entreprises d'audit, telles que les *Big Four*[40], ont développé de vastes programmes de formations en matière de LBC/FT à destination des entités assujetties et sont régulièrement recrutées par certaines pour effectuer les évaluations globales ou fournir des conseils en matière de conformité. Autre dépense conséquente, les systèmes de détection automatiques des transactions atypiques sont devenus plus que jamais nécessaires au bon fonctionnement des dispositifs LBC/FT compte tenu du rôle qu'ils jouent dans le contrôle de première ligne. Comme nous l'a expliqué l'expert durant l'interview, les logiciels de *monitoring* et de *screening* représentent un investissement important et souvent inévitable pour les institutions financières. De ce fait, elles se retrouvent dans une position délicate où le risque de collusion tacite entre les fournisseurs de ces logiciels est présent. Si ceux-ci s'accordent pour augmenter fortement les prix du marché, cela pourrait, avec le temps, porter préjudice aux institutions. In fine, le développement de la règlementation et de la législation actuelle en matière de LBC/FT a favorisé l'essor du secteur de la conformité, qui stimule désormais les investissements des entités en leur fournissant des produits et services toujours plus évolués. En effet, pour des raisons évidentes de rendement, les banques ne veulent pas se trouver au premier rang des investissements dans ce domaine mais elles ne veulent pas non plus y figurer dernières. De ce fait, la référence de conformité est, d'une part, prescrite par la manière dont les autorités de contrôle supervisent les dispositifs LBC/FT, et, d'autre part, imposée par la qualité – et donc les prix – des activités et services fournis par ce secteur. (VERHAGE, 2014, pp.121-135).

Dans un monde où les nouvelles technologies telles que les Fintechs renforcent un peu plus la concurrence bancaire, comment les institutions financières « classiques » peuvent-elles faire face à leurs obligations réglementaires en matière de LBC/FT et, en même temps, maintenir un bon niveau de satisfaction chez leurs clients, qui recherchent des produits de moins en moins chers, voir complètement gratuits ?

Les obligations de vigilance et de déclaration instaurées par la Loi du 18 septembre 2017 renforcent la responsabilité des entités assujetties dans la lutte contre le blanchiment et le financement du terrorisme. À l'aide de dispositifs de LBC/FT efficaces, les entités ont le pouvoir d'empêcher la propagation de ces phénomènes dans le secteur financier et dans la société en général. Les statistiques de la CTIF révèlent que les institutions financières introduisent plusieurs milliers de déclarations de soupçon chaque année (CTIF, 2018, p.41), ce qui nous porte à croire qu'elles participent de façon conséquente à la LBC/FT en Belgique.

[40] Expression utilisée pour désigner les quatre plus grands groupes d'audit financier au niveau mondial : Deloitte, EY (Ernst & Young), KPMG et PwC (PricewaterhouseCoopers).

Toutefois, si l'on continue l'examen de ces statistiques publiées par la CTIF, il semble que certaines professions plutôt sensibles, telles que les agents immobiliers ou les avocats, ne sont pas encore parfaitement conscientes de l'importance des responsabilités qui leur incombent. Comme expliqué précédemment (Cf. Chapitre 1), le marché immobilier est utilisé de façon récurrente par les blanchisseurs pour réintégrer les capitaux illicites dans l'économie légale. Cependant, la CTIF ne dénombre qu'une cinquantaine de déclarations effectuées par les agents immobiliers en 2018 (CTIF, 2018, p.41). Le constat est encore plus alarmant du côté des avocats qui n'ont transmis que 8 déclarations, ce qui représente 0.02% du nombre total de déclarations transmises à la Cellule en 2018 (CTIF, 2018, p.41). Le GAFI faisait déjà cette constatation en 2015 et pointait particulièrement les secteurs des avocats et des diamantaires (FATF-GAFI, 2015b, p.8). Cette quasi-absence de déclaration de la part des avocats a été abordée durant l'interview avec notre expert qui l'expliquerait, d'une part, par les dérogations à certaines obligations accordées à cette profession[41] et, d'autre part, par le lien commercial direct qui existe entre l'avocat et son client. Imaginons qu'un avocat indépendant, constitué en société mais étant la seule personne physique à la tête de celle-ci, dénonce une personne pour blanchiment ou financement du terrorisme. Il ne peut, dès lors, plus l'accepter comme cliente et perd ainsi une partie de son « gagne-pain » ce qui pourrait, dans certains cas, mettre sa société en mauvaise posture. À l'inverse, les procédures de LBC/FT des institutions financières sont généralement assurées par la fonction de *Compliance* – caractérisée pour son indépendance par rapport aux autres fonctions de l'institution et axée, entre autres, sur l'intégrité des activités bancaires – et elles ont l'obligation de mettre en place un système d'alerte (*whistleblowing*[42]*)* interne permettant à tous leurs collaborateurs de dénoncer par une voie spécifique, indépendante et anonyme des infractions à la Loi anti-blanchiment (BNB, 2019). La combinaison de ces observations démontre une faille dans le dispositif belge où l'on pourrait craindre que ces professions réputées « sensibles » soient exploitées par les blanchisseurs qui se sentent de plus en plus contrôlés par le secteur financier.

8.2. Le *de-risking*

Au vu du nombre d'obligations en matière de LBC/FT auxquelles les institutions financières sont déjà tenues, elles peuvent aujourd'hui être tentées de se séparer de certains clients à risque ou d'éviter d'entrer en relation d'affaire avec ceux-ci dans le but de se dispenser des contraintes afférentes à une

[41] En effet, la Loi précise que « […] les informations connues de l'avocat à l'occasion de l'exercice des activités essentielles de sa profession, […], à savoir l'assistance et la défense en justice du client, ainsi que le conseil juridique, même en dehors de toute procédure judiciaire, demeurent couvertes par le secret professionnel. Elles ne peuvent donc pas être portées à la connaissance de la CTIF. » (Loi du 18 septembre 2017, Art.52)

[42] Dénonciation en anglais

surveillance accrue desdits clients (BUYLE et CLOQUET, 2016). Le *de-risking*[43] apparait donc lorsqu'une institution financière décide de restreindre ou cesser des relations commerciales avec certaines catégories de clients pour éviter, au lieu de gérer, le risque conformément à la RBA prônée par le GAFI. Les institutions qui se tournent vers ce genre de pratique le font généralement par souci de rentabilité, pour éviter les obligations prudentielles ou encore pour limiter le risque de réputation qu'elles encourent. (OCDE, 2019b)

Cette pratique pose un problème évident de financement pour les catégories de clients réputées à risque, qui se voient refuser l'accès au monde financier « classique ». Dès lors, ces clients auront tendance à se tourner soit vers des établissements bancaires plus petits – qui souvent disposent de moins de moyens de surveillance des clients à haut risque – soit vers des marchés financiers alternatifs – moins régulés et plus anonymes, voire opaques, que leurs équivalents classiques. Le *de-risking* met alors en lumière un certain paradoxe dans le système de LBC/FT actuel où les autorités ne cessent d'accroitre la sévérité des législations LBC/FT pour mieux combattre ces deux criminalités mais encouragent involontairement l'utilisation de canaux moins contrôlés et moins transparents. (DEBRUYNE, 2019)

Au cours d'une séance d'information organisée par la BNB en novembre 2019, Jean HILGERS, actuel directeur de la Banque, dévoilait certains sujets d'actualité sensibles en matière de LBC/FT dont le *de-risking*. Il rappelle dans sa présentation que même si une banque n'a pas l'obligation générale d'accepter tous les clients, chaque décision concernant l'entrée en relation d'affaire – ou l'exécution d'une opération occasionnelle – doit faire l'objet d'une évaluation individuelle, d'une analyse et d'une justification au cas par cas. Les refus de nouer une relation avec un client potentiel doivent également être correctement justifiés par l'institution pour éviter ainsi toute sorte de pratique discriminatoire envers certaines catégories de clients, pratique contraire aux lois et règlements en matière de services bancaires de base[44]. (BNB & CTIF, 2019)

La décision de clôture d'une relation suite à une déclaration de soupçon doit également être prise sur base de l'évaluation individuelle du client et de l'ensemble des informations à disposition de l'institution. La BNB insiste sur le fait qu'une décision de principe de rompre de manière systématique la relation après une déclaration est non seulement contraire au Règlement mais pourrait surtout laisser entendre indirectement et implicitement au client qu'une déclaration de soupçon le concernant a été adressée à la CTIF. (GATOT, 2019)

---

[43] Atténuation des risques en anglais

[44] Comme l'Art.VII.55/12 du Code de Droit économique qui stipule que « *L'établissement de paiement a un accès objectif, non discriminatoire et proportionné aux services de comptes de paiement des établissements de crédit. […]* »

Pour lutter contre ce phénomène de *de-risking*, le directeur de la BNB explique également que les frais engendrés peuvent être répercutés sur les clients sous forme d'honoraires pour autant qu'ils soient « objectifs et proportionnés », ce qui réduirait une partie non-négligeable des coûts liés aux clients à risque. En outre, la Banque interpelle les institutions financières sur l'importance d'engager un dialogue pour rétablir la confiance en formalisant les critères à prendre en compte pour l'analyse individuelle à effectuer. (BNB & CTIF, 2019)

8.3. Les technologies en constante évolution

Dans le monde connecté que nous connaissons aujourd'hui, les avancées en matière d'innovation technologique ont incité de nombreux domaines à se réinventer et le secteur financier n'a pas échappé à la règle. Entre l'explosion du marché des cryptos-actifs, le développement continu des systèmes de paiements en ligne ou encore l'émergence de l'intelligence artificielle dans la détection des transactions suspectes, les nouvelles technologies incitent les acteurs financiers, les législateurs et même les cellules de renseignement à repenser leurs approches pour lutter le plus efficacement possible contre le blanchiment et le financement du terrorisme.

Les risques de blanchiment et de financement du terrorisme liés aux cryptos-actifs[45] sont assez élevés en raison de leur vocation de « cash numérique » mais surtout de l'anonymat qu'ils procurent aux utilisateurs. Aujourd'hui, certaines plateformes proposent d'échanger différents crypto-actifs entre eux, ce qui permet ainsi aux criminels de convertir des cryptos-actifs reposant sur des *blockchains*[46] traçables – comme le célèbre Bitcoin – en crypto-actifs reposant sur des *blockchains* intraçables qui garantissent alors l'anonymat des transactions (TRACFIN, 2018, p.57). Une fois ces crypto-actifs devenus intraçables, ils peuvent dès lors jouer un rôle prépondérant dans les circuits de BC/FT en étant par exemple utilisés sur le *Dark Net* pour acheter des biens illicites comme des stupéfiants ou des armes. Pour les activités légitimes du secteur des crypto-actifs, l'enjeu actuel consiste à éviter de manipuler des fonds en cours de blanchiment, ce qui requiert l'application de mesures de vigilance. Si aujourd'hui l'apparition des crypto-actifs dans les déclarations de soupçon faites à la CTIF est encore très faible, cette traçabilité limitée des flux financiers pourrait à l'avenir poser un réel problème dans la LBC/FT.

[45] Le terme « crypto-actifs » a été choisi par la BNB parce qu'elles estiment que les crypto-monnaies ne sont pas comparables à de l'argent émis par une banque centrale ou une autorité publique et que certains crypto-actifs n'ont pas pour objectif d'offrir une alternative aux monnaies existantes. (Circulaire de la BNB publiée le 19 juillet 2019, p.3)

[46] Technologie de stockage et de transmission d'informations hébergée par une partie des utilisateurs, fonctionnant ainsi sans organe central de contrôle et sécurisée par cryptographie.

Au vu de l'essor mondial des cryptos-actifs, ce n'est pas un phénomène qui devrait prendre fin dans un futur proche. Par conséquent, les législateurs travaillent ardemment sur l'élaboration des normes concernant les sociétés opérant dans ce domaine. En juillet 2019, la BNB a déjà fait un premier pas vers la régulation des activités liées à ces technologies au travers d'une Circulaire dans laquelle elle demande aux établissements exposés aux crypto-actifs d'exercer « une vigilance accrue » envers ce type d'expositions et de services (Circulaire de la BNB publiée le 19 juillet 2019, p.2). Toutefois, en Belgique, les plateformes d'échanges de monnaies virtuelles et les fournisseurs de portefeuilles de stockage ne sont toujours pas régulés et, de ce fait, ces entités ne sont pas soumises au dispositif de LBC/FT belge.

Cette situation devrait s'améliorer prochainement avec la transposition en droit national de la 5ème Directive anti-blanchiment, publiée le 19 juin 2018, prévue pour le 10 janvier 2020 au plus tard. Les nouvelles dispositions concernant les plateformes d'échange de monnaies virtuelles règlementent les échanges entre monnaies fiduciaires et crypto-monnaies, appelés « fiat-to-crypto », mais ne traitent pas de la question des échanges de monnaies virtuelles entre elles, appelés « crypto-to-crypto ». Certes, cette nouvelle règlementation anti-blanchiment apporte déjà quelques solutions aux difficultés rencontrées jusqu'à présent avec les crypto-actifs mais ne comblera malheureusement pas l'ensemble des lacunes actuelles. Finalement, il est important de souligner que le contrôle de ces prochaines entités assujetties va certes faciliter le travail des autorités de LBC/FT, en leur offrant une vision plus claire du secteur et de nouvelles collaborations avec les acteurs de ce marché, mais augmentera aussi la confiance des utilisateurs de ces crypto-actifs. (CTIF, 2018, p.25)

Les paiements en ligne sont une autre technologie installée aujourd'hui au cœur de la vie quotidienne. Ceux-ci sont assurés par ce que l'on appelle des prestataires de services de paiement [ci-après PSP] qui sont des tiers offrant aux commerçants (marchands, ONG, site internet) la possibilité d'accepter, de manière transparente, des paiements en ligne effectués généralement par carte bancaire ou carte de crédit. Parmi les plus connus, nous pouvons par exemple citer PayPal ou AmazonPayments. Sachant que les réseaux de blanchiment et de terrorisme cherchent de plus en plus à se détourner du système bancaire classique, ces établissements de paiement et de monnaie électronique en ligne, dont les procédures de vérifications sont moins robustes et le contrôle par les autorités de supervision moins établi, deviennent une cible pour les criminels (TRACFIN, 2018, p.41)

Au vu du nombre croissant de paiements électroniques générés chaque année en Europe, le législateur européen avait déjà réagi en 2015 en adoptant une nouvelle directive (2015/2366) concernant les services de paiements, appelée la directive DSP 2. Transposée en droit national au travers de la Loi

du 11 mars 2018[47], elle renforce notamment l'authentification des clients. Dorénavant, l'identité devra être validée à l'aide de deux des trois caractéristiques suivantes : quelque chose de connu du client comme son code pin, quelque chose en la possession du client comme son smartphone et quelque chose propre au client telle que son empreinte digitale (FEBELFIN, 2019). Faisant partie intégrante du système financier actuel, les PSP sont désormais soumis aux obligations en matière de LBC/FT en tant qu'entité assujettie de la Loi *AML*.

Toutefois, un des risques de BC/FT identifiés par la CTIF en dans le secteur de PSP est lié aux cartes de paiement électronique rattachées à des portes-feuilles en crypto-monnaies. La Cellule explique que « *ces cartes remplissent les mêmes fonctions qu'une carte de paiement classique mis à part le fait que les fonds disponibles correspondent à la contre-valeur en monnaie fiduciaire du montant de crypto-monnaies acquis par le détenteur de la carte* ». Ce système « crypto-to-plastic » représente un risque de BC/FT potentiel dans la mesure où ces transactions – retrait d'espèces ou paiements en ligne – ne transitent pas par un établissement financier proposant des produits de type monnaies fiduciaires et ne sont donc pas soumises aux vérifications du dispositif de LBC/FT puisqu'en l'absence de ce maillon de la chaine, les blanchisseurs restent dans un environnement crypto-to-crypto. (CTIF, 2018, p.26)

Au vu des risques présentés supra, nous pourrions souhaiter que la transposition en droit national de la 5ème Directive aille plus loin et régule de manière plus complète le secteur des crypto-actifs en étendant les obligations de vigilance aux échanges crypto-to-crypto. Ces échanges sont, rappelons-le, un élément fondamental des chaines de blanchiment où les monnaies virtuelles transparentes sont blanchies via des crypto-actifs intraçables. (CTIF, 2018, p.25)

Néanmoins, il est également important de noter que les évolutions technologiques peuvent aussi être une source de progrès pour la LBC/FT notamment au niveau des outils de contrôle des transactions. Nous en avons déjà parlé plusieurs fois au cours de ce travail, ces programmes de *monitoring* et de *screening* sont maintenant complètement intégrés dans les dispositifs de LBC/FT, que ce soit au niveau des entités assujetties ou encore des autorités de contrôle telles que la CTIF ou l'OCAM.

À l'heure actuelle, une grande majorité des systèmes de contrôle des transactions s'appuient sur des scénarios de détection des opérations atypiques. Comme l'explique l'expert que nous avons interrogé, ces scénarios sont en fait pré-paramétrés et adaptés selon des règles et des critères assez fixes,

[47] Loi relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement

définis au préalable par l'établissement financier. Bien souvent, la modification de ces scénarios entraine des frais supplémentaires pour les utilisateurs du système qui évitent donc les actualisations trop fréquentes. Lorsque les alertes sont générées par le système, elles sont traitées par des analystes spécialisés en matière de LBC/FT. Cependant, l'évolution permanente des législations et des règlements a nettement augmenté le volume d'alertes à traiter ainsi que le nombre de faux positifs à éliminer, faisant ainsi chuter le taux d'efficacité du dispositif de LBC/FT mis en place. En outre, la difficulté d'ajustement de ces systèmes de contrôle ne permet pas toujours l'identification des nouvelles typologies ou des nouveaux schémas de criminalité financière. Les outils actuels fonctionnent donc sur base de données du passé, ce qui remet en cause la pertinence des dispositifs mis en place pour faire face aux évolutions des risques BC/FT. (AUBRY, 2019)

Les progrès réalisés en matière d'Intelligence Artificielle [ci-après IA] ces dernières années pourraient apporter certaines solutions aux différents problèmes identifiés ci-dessus et offrir aux entités assujetties des dispositifs de LBC/FT suffisamment flexibles et robustes pour assurer une détection des risques efficace tout en minimisant les moyens techniques et humains nécessaires. Un des champs d'étude de l'IA, le *machine learning*, combine différentes approches statistiques et mathématiques qui donnent aux ordinateurs la capacité « d'apprendre » à partir de données et d'informations observées pour élaborer ainsi des modèles prédictifs. Nous ne rentrerons pas dans les détails techniques propres à cette technologie mais nous allons cependant développer ses atouts dans le cadre de la LBC/FT. Par exemple, lorsque ces techniques d'apprentissage sont supervisées, l'outil est capable de définir des catégories d'alerte et leurs priorités de traitement associées en se basant sur les alertes passées et la manière dont elles ont été traitées. Ces catégories sont perpétuellement mises à jour par les algorithmes puisque le flux de données des transactions est continu. L'apprentissage devient alors « automatique » et les catégories s'adaptent aux nouvelles tendances de BC/FT observées dans les opérations financières. Avec ce principe de catégorisation, chaque alerte générée est tout d'abord priorisée et ensuite redirigée vers le processus de prise en charge le plus adapté en fonction de sa catégorie. Cette application de *machine learning* répond complètement aux exigences de l'approche fondée sur les risques puisqu'elle permet un traitement plus rapide et plus adapté pour les alertes hautement prioritaires. Un autre facteur d'adoption du *machine learning* dans la LBC/FT est la capacité des infrastructures informatiques à traiter de grands volumes de données tels que les flux de transactions des institutions financières, la base de données de la clientèle ou encore les listes nationales et internationales regroupant les PPE. En outre, des techniques récentes permettent désormais de connaitre, pour chaque alerte générée, les variables ayant conduit à la décision proposée et leur contribution, ce qui facilite l'analyse des transactions atypiques et augmente leur explicabilité. (AUBRY, 2019)

Au niveau des autorités de contrôle, la BNB a émis un avis plutôt positif sur ces différentes évolutions technologiques liées notamment à l'IA qu'elle reconnait comme de potentielles sources de progrès et se dit « *ouverte à accompagner les parties prenantes dans le cadre du développement initial de projets* » (BNB & CTIF, 2019). Alors pourquoi les possibilités offertes par l'IA ne sont-elles pas encore pleinement exploitées par les institutions ? Dans l'esprit collectif, les mots intelligence artificielle renvoient souvent à la complexité et à l'élitisme alors que l'IA est omniprésente dans nos vies quotidiennes (logiciels de reconnaissance vocale, montres connectées, domotique). Même si les institutions financières sont bien conscientes des opportunités offertes par ces évolutions technologiques et surtout des avantages concurrentiels qu'elle peut leur procurer, la plupart d'entre elles sont encore très hésitantes et commencent seulement les phases de test pour lancer des projets intégrant l'IA, confirmant le sentiment d'élitisme évoqué plus haut. (DE BONY, 2019)

L'exemple de *machine learning* développé ci-dessus n'est qu'une faible représentation des possibilités offertes par l'IA dans la LBC/FT. Il n'empêche que l'introduction de ces nouvelles technologies dans les dispositifs de lutte permettrait de focaliser les ressources sur l'analyse de cas plus complexes, revalorisant ainsi les métiers d'analystes *AML* qui exigent expertise et technicité. Finalement, ces évolutions technologiques pourraient, dans le futur, permettre aux acteurs de la LBC/FT de rencontrer parfaitement les attentes de l'approche fondée sur les risques qui, pour rappel, vise une allocation optimale des ressources en vue d'atteindre une efficacité aussi grande que possible de la prévention des risques de BC/FT.

8.4. L'efficacité de la chaîne de LBC/FT

La chaîne de LBC/FT débute avec l'implication des entités assujetties qui sont supposées repérer les transactions suspectes dans le cadre de leurs activités quotidiennes. Ce devoir de signalement exige une connaissance approfondie et un examen régulier des risques de BC/FT auxquelles elles sont confrontées. C'est une des raisons pour lesquelles les entités sont tenues de réaliser de façon périodique une évaluation globale de leurs risques. Se basant sur l'article 17 de la Loi (Cf. Annexe 6, L'évaluation globale des risques dans la Loi AML), la BNB estime que le BWRA doit être mis à jour « *chaque fois que se produisent des événements notables, tant en leur sein que dans leur environnement, qui sont susceptibles de modifier de manière significative la nature et l'ampleur des risques de BC/FT ou leur évaluation* ».

En pratique, la Banque demande aux institutions financières de mettre à jour leur BWRA au moins tous les deux ans et insiste sur cette obligation. Un grand nombre de décisions propres à l'entité peut générer des modifications de son exposition aux risques : le développement de nouveaux canaux de distribution comme l'E-Banking, l'extension de ses opérations dans des pays étrangers, où, par,

exemple, les réglementations en matière de LBC/FT sont moins rigoureuses, l'ouverture à de nouveaux secteurs d'activités réputés plus sensibles, etc. Il se peut également que des événements externes viennent influencer les risques BC/FT ou leur évaluation. Parmi ceux-ci, nous pouvons notamment citer les modifications du cadre légal et règlementaire national ou international, l'émergence de nouvelles formes de criminalités, l'apparition de nouvelles typologies ou encore des modifications importantes du contexte socio-économique sans oublier les avancées en matière d'innovation technologique dans le secteur financier. (BNB, 2019)

Aujourd'hui, avec la mondialisation financière qui cherche constamment à améliorer la liberté et surtout la vitesse de circulation des fonds, les mesures de contrôle et de vérification mises en place auront toujours un temps de retard. Ce temps intermédiaire représente l'espace d'action des blanchisseurs et des partisans du terrorisme. (KOUTOUZIS & THONY, p.121) Dès lors, il appartient aux entités assujetties d'agir afin de réduire cet espace en mettant régulièrement à jour leurs processus de LBC/FT. L'actualisation constante du BWRA apparait ainsi comme une condition sine qua non pour assurer l'efficacité du dispositif de LBC/FT mis en place, tout comme le respect de l'ensemble des obligations imposées aux entités assujetties. En tant que premier maillon de la chaîne de LBC/FT, elles doivent acquérir les capacités, outils et compétences nécessaires à la détection des opérations atypiques. Les milliers de déclarations de soupçon envoyées chaque année à la CTIF attestent d'une certaine contribution de la part des entités au processus de LBC/FT. Toutefois, il est bon de se demander si les résultats obtenus sont proportionnels aux efforts fournis ?

Pour rappel, la finalité ultime de la CTIF est la transmission d'indices sérieux de blanchiment ou de financement du terrorisme aux autorités judiciaires. Dans le cadre de l'évaluation de la chaîne de LBC/FT, il est intéressant de se pencher sur l'efficacité de la Cellule dans le traitement des déclarations reçues en analysant, entre autres, la manière dont elle traite ces déclarations et certaines statistiques publiées dans son rapport annuel. Le processus de prise en charge des déclarations reçues par la CTIF est basé sur leur degré d'importance (montant en cause, nature des opérations, présence de PPE) et sur leur niveau de priorité (urgence lorsque des fonds peuvent encore être bloqués ou saisis, instruction judiciaire en cours) pour déterminer l'ampleur et la rapidité à mettre en place pour ses recherches. En 2018, la CTIF a reçu 33 445 déclarations de soupçon provenant des entités assujetties, des CRF étrangères et d'autres autorités compétentes telles que le SPF Finances ou le service des douanes et accises. Après analyse de ces informations suspectes, 2 972 déclarations ont été transmises aux autorités judiciaires[48], soit un peu moins de 10% du nombre de déclarations reçues initialement. (CTIF, 2018,

[48] La CTIF ne transmet pas de copie des déclarations de soupçon mais uniquement les éléments relatifs aux opérations suspectes que celles-ci contiennent, enrichis de son analyse. (CTIF, 2018, p.40)

pp.38-42) Même si cette différence s'explique en partie par la présence d'un grand nombre de déclarations automatiques, le GAFI remet en question ce processus dans lequel il estime que « *les classements par opportunité sont trop nombreux, atténuant le taux de la réponse pénale* » (FATF-GAFI, 2015b, p.15).

Lorsque l'on continue l'analyse des statistiques publiées par la CTIF, nous pouvons constater que sur les 5 110 dossiers transmis aux autorités judiciaires entre janvier 2014 et décembre 2018, 39 dossiers ont fait l'objet d'une condamnation. Toutefois, il faut prendre en compte le fait que certains dossiers sont encore récents et laisser le temps aux magistrats de les traiter. Actuellement, l'information judiciaire est en cours pour approximativement 80% des dossiers transmis par la Cellule tandis que 20% ont déjà été classés sans suite. (CTIF, 2018, p.62) Dans son rapport d'évaluation mutuelle publié en 2015, le GAFI a largement critiqué l'efficacité du système judiciaire belge en matière de BC/FT. Il souligne, entre autres, le manque de ressources, de moyens matériels, de formations et de coordination des autorités pénales à tous les niveaux et la longueur excessive de certaines procédures, qui entraine parfois la prescription de poursuites et l'atténuation des sanctions. L'absence au niveau national d'une stratégie judiciaire définie en matière de BC/FT et de coordination entre les magistrats limite la portée des actions de LBC/FT. Ce manquement impacte directement l'efficacité de la détection, de la poursuite et de la sanction des opérations de blanchiment ou de financement du terrorisme plus complexes. (FATF-GAFI, 2015b, pp. 9-15) Selon le juge d'instruction spécialisé en matière financière, Michel Claise, 90% des dossiers transmis par la CTIF au parquet de Bruxelles ne sont pas examinés principalement par manque de ressources humaines, que ce soit au niveau des magistrats spécialisés ou des enquêteurs de la police fédérale. Il estime que le gouvernement belge est loin de faire de la LBC/FT une priorité absolue alors que l'ampleur de la fraude ne fait qu'augmenter au fil des années. (RTBF, 2018)

In fine, même si les spécialistes reconnaissent que l'arsenal législatif belge récemment mis en place est efficace pour lutter contre le blanchiment et le financement du terrorisme, qu'en est-il des moyens humains mis en œuvre pour appliquer la loi ?

8.5. Les pistes de solutions

Plusieurs améliorations du dispositif belge de LBC/FT pourraient répondre aux enjeux développés supra. Toutefois, nous pensons que pour améliorer de manière efficace la lutte contre ces deux phénomènes, l'implication de l'ensemble des acteurs de la chaîne de LBC/FT en Belgique est nécessaire.

À la tête du dispositif de LBC/FT en Belgique, nous retrouvons tout d'abord le législateur. Un peu plus de deux ans après l'entrée en vigueur de la Loi du 18 septembre 2017, celle-ci devrait

normalement être revue en 2020 en vue de la transposition en droit national de la 5ème Directive qui concerne notamment les crypto-actifs. Comme expliqué à la section 8.3, la législation belge pourrait décider de légiférer également les échanges crypto-to-crypto, transactions récurrentes dans les chaines de blanchiment. Cette mise à jour législative devrait également intégrer certaines mesures concernant les dernières tendances et typologies de BC/FT détectées par la CTIF. En outre, si le législateur favorisait l'utilisation des nouvelles technologies telles que l'IA dans la LBC/FT, il pourrait avoir un impact indirect sur le secteur de la conformité qui développerait alors de nouveaux outils de *screening* et de *monitoring* construits autour de ces technologies prometteuses. À partir du moment où divers processus d'IA seront directement intégrés dans les logiciels achetés par les institutions financières, nous pouvons espérer qu'ils deviendront progressivement la norme pour un grand nombre d'entités assujetties.

Ensuite, l'implication des autorités de contrôle dans une approche encore plus proactive améliorerait la qualité des dispositifs de lutte mis en place par les entités assujetties. En augmentant l'étendue, la fréquence et l'intensité de leurs contrôles, adaptés au niveau d'exposition aux risques de BC/FT des entités, les lacunes constatées dans les différents dispositifs de lutte mis en place actuellement pourraient être atténuées. Il serait également primordial que les autorités continuent et perfectionnent encore leurs procédés de retours d'informations qui permettent aux entités de « s'autocorriger », d'améliorer leurs politiques, procédures et mesures en matière de LBC/FT et d'avoir une idée plus précise sur ce que les autorités attendent concrètement d'elles.

Dans le volet préventif, la CTIF a un rôle important à jouer en tant que vecteur d'information. Plus elle communiquera avec les entités assujetties et la population sur l'intérêt de la lutte, sur les effets collatéraux du BC/FT et sur le bien-fondé d'appliquer la Loi, mieux ils comprendront l'importance des déclarations, qui ne doivent ni être considérées comme un procédé automatique (ex. les déclarations de couvertures), ni comme un procédé exceptionnel (ex. déclarations provenant des avocats). De plus, la mise en place de *feedbacks* sur les déclarations de soupçons reçues devrait encore être renforcée lors des formations ou séances d'informations données par la CTIF permettant ainsi une meilleure compréhension dans la détection et la déclaration des opérations liées au blanchiment et/ou au financement du terrorisme.

Concernant les entités assujetties, il est évident que le respect de leurs obligations en matière de LBC/FT renforce le dispositif de lutte mis en place en Belgique. Toutefois, il est également important qu'elles continuent à mettre à jour de façon périodique leur exercice d'évaluation globale des risques. Cette actualisation, attendue au minimum tous les deux ans, permettrait de maintenir un certain niveau

d'efficacité des mesures de lutte mises en place, non seulement au niveau des entités assujetties mais également au niveau de l'évaluation nationale des risques.

Finalement, nous avons constaté que les autorités judiciaires belges manquaient cruellement de moyens pour assumer leurs responsabilités dans la chaîne de LBC/FT. Elles ont besoin d'engager plus de ressources humaines, notamment des magistrats et des enquêteurs, et d'obtenir plus de moyens financiers pour former de manière continue leurs employés spécialisés dans la LBC/FT. En effet, pour mettre en place un processus d'enquête efficace, leurs compétences devraient être mises à jour de façon régulière en fonction des nouvelles typologies à détecter, analyser et poursuivre dans les affaires liées au blanchiment ou au financement du terrorisme. Par ailleurs, il serait également intéressant de revoir l'ensemble des procédures relatives aux sanctions financières liées au terrorisme, à son financement et à la prolifération des armes de destruction telles que le gel des actifs concernés. Actuellement, le délai entre la prise de décision d'une sanction par l'ONU et son application effective en Belgique est de 2 à 4 jours. Le processus décisionnel belge est reconnu comme trop lent par le GAFI pour que ces sanctions soient appliquées de manière efficace, c'est-à-dire « sans délai », et nécessiterait donc des mesures d'améliorations dans le futur.

CONCLUSION

Au cours de ce travail, nous avons voulu commencer par mettre en évidence la nécessité de la lutte contre le blanchiment des capitaux et le financement du terrorisme. Ces deux phénomènes, toujours en progression, constituent une réelle menace pour la société et la démocratie au travers du financement de nombreuses activités criminelles et de l'augmentation de la criminalité à col blanc.

La réponse mondiale apportée par les recommandations du GAFI et les instruments d'autres organisations internationales, telles que le FMI ou l'Union Européenne, affirme la légitimité de cette lutte depuis bientôt trente ans. L'engagement politique des États a permis, au fil du temps, de converger vers des règlementations homogènes en matière de blanchiment de capitaux et de financement du terrorisme, favorisant ainsi la coopération internationale entre les différentes cellules de renseignements financiers et impliquant de plus en plus d'acteurs dans la lutte.

L'approche fondée sur les risques peut être vue comme un des aboutissements d'une succession de législations et d'initiatives internationales qui, face à l'évolution constante des techniques de blanchiment, nécessitaient davantage de souplesse dans leurs procédures préventives. Elle permet aux acteurs de la lutte d'adapter leurs mesures de prévention contre le BC/FT en fonction des risques auxquels ils sont exposés, visant ainsi une allocation optimale des ressources. Instaurée en Belgique par la Loi du 18 septembre 2017, la mise en œuvre de l'approche fondée sur les risques a notamment été transposée à travers l'obligation pour les entités assujetties de réaliser une évaluation globale des risques qui leur sont propres.

L'analyse de la mise en place de cette évaluation au sein d'un établissement de crédit, nous a permis d'avoir une vision concrète plus précise sur le BWRA et sur son processus de réalisation. L'étude de cas donne un premier aperçu des coûts générés par l'entrée en vigueur de la Loi, tels que les investissements en ressources humaines et technologiques, mais met également en lumière les avantages apportés à l'entité étudiée. D'abord, les obligations de chaque entité sont désormais clairement définies, permettant ainsi à l'établissement de vérifier plus facilement la conformité de son dispositif de lutte. Ensuite, la réalisation du BWRA offre, en un seul exercice, une vue globale sur les risques propres à l'établissement, les mesures qui s'y rapportent, leur niveau d'adéquation et, le cas échéant, sur les mesures de correction nécessaires avec leur calendrier de mise en place. De plus, l'actualisation de cette évaluation permet à l'établissement étudié de maintenir un dispositif de lutte efficace et adapté aux nouveaux risques auxquels il est exposé. L'application de l'approche fondée sur les risques a également modifié l'analyse des opérations suspectes, qui sont maintenant déclarées à la CTIF dès qu'il y a un soupçon de la part de la banque, peu importe le montant de la transaction concernée. Enfin, nous avons

pu relever l'utilité du principe de proportionnalité, qui demande à l'entité étudiée de développer des politiques et des procédures en matière de lutte anti-blanchiment et anti-financement du terrorisme adaptées à sa taille et sa nature.

Après avoir étudié le cas particulier d'un établissement de crédit, nous nous sommes intéressés aux évaluations globales réalisées jusqu'à présent par l'ensemble des entités assujetties placées sous l'autorité de la BNB. Alors que certaines entités ont déjà effectué plusieurs BWRA de qualité, d'autres n'ont pas encore pris conscience ni de la finalité, ni de l'importance de cet exercice, réalisant alors leur évaluation dans un simple objectif de conformité règlementaire au lieu de se livrer à un réel examen critique de leur dispositif de lutte. Aujourd'hui, cette situation amène une grande disparité quant au degré de pertinence des évaluations globales, des analyses des gaps et des plans d'actions réalisés par les différentes institutions financières. Pour y remédier, la BNB a demandé aux institutions financières de réexaminer et surtout de mettre à jour leur BWRA. Elle attend de cette actualisation une réelle amélioration des évaluations globales, qualifiées jusqu'à présent de « perfectibles ».

Malgré l'ensemble des actions positives mises en place par la Belgique, il reste encore une série d'enjeux importants dans le dispositif belge de LBC/FT.

Premièrement, les nombreuses obligations imposées aux professionnels assujettis ont fait naître une dualité dans leurs relations d'affaire, où elles doivent exercer leur fonction dans le cadre commercial de leurs activités tout en respectant le cadre réglementaire de la LBC/FT. En effet, les obligations de vigilance à l'égard de la clientèle peuvent parfois nuire à leurs relations avec certains clients, qui se sentent surveillés, mais également compliquer l'extension de leurs activités à certains canaux dont les mesures d'identification sont plus difficiles à mettre en place. De plus, les institutions financières investissent considérablement dans le secteur de la conformité, devenu progressivement l'étalon de mesure définissant, avec les autorités de contrôle, si oui ou non un dispositif de LBC/FT est efficace et créant ainsi une forme de dépendance envers les biens et services fournis par ce secteur. Ces dépenses représentent encore un nouveau défi pour les institutions financières qui doivent continuer à honorer leurs obligations règlementaires tout en offrant à leurs clients des produits à des prix concurrentiels. Cette dualité dans les relations d'affaire pose également problème pour certaines professions reconnues comme sensibles aux risques de blanchiment ou de financement du terrorisme, telles que les avocats ou les agents immobiliers, où l'on observe une quasi-absence de déclarations de soupçons due aux pertes financières que celles-ci pourraient engendrer pour leur société. Créant ainsi une faille dans le système de surveillance, ces professions réputées plus sensibles risquent d'être exploitées par les criminels, qui se sentent de plus en plus contrôlés par les institutions financières en général plus sévères.

Deuxièmement, les pratiques de *de-risking* posent aujourd'hui un important problème de financement pour certaines catégories de clients, réputées « à risques », qui sont écartées par les

institutions financières « classiques » afin d'éviter les contraintes liées à une surveillance accrue de ces clients. Lesdits clients ont alors tendance à se tourner vers des systèmes de financement moins contrôlés et moins transparents, démarche involontairement provoquée par la sévérité des législations anti-blanchiment et anti-financement du terrorisme.

Troisièmement, l'explosion des nouvelles technologies est en train de révolutionner le secteur financier et, par conséquent, d'ouvrir de nouvelles possibilités de fraude pour les criminels qui utilisent, entre autres, le marché des crypto-monnaies et certains systèmes de paiements en ligne. Ces nouveaux moyens de paiements, encore trop peu régulés en Belgique actuellement, entraînent le développement d'une économie parallèle au système financier « classique », propice aux transactions illicites qui permettent ainsi de blanchir des capitaux et de financer toutes sortes d'activités illégales telles que le terrorisme.

De plus, ces avancées en matière d'innovation technologique nous rappellent, deux ans après son introduction, l'importance de l'actualisation de l'évaluation globale des risques. Comme nous l'avons constaté tout au long de cette étude, de nombreux facteurs influencent l'exposition des entités aux risques de BC/FT. Malheureusement, nous savons par expérience que la législation aura toujours un temps de retard, léger ou important, sur les nouvelles techniques des blanchisseurs. En actualisant leur BWRA de façon régulière, les entités pourraient déjà réduire l'écart qui existe entre les dernières typologies de blanchiment et de financement du terrorisme décelées par les autorités compétentes et les dispositifs mis en place.

Finalement, l'efficacité de la chaîne de LBC/FT en Belgique est encore à améliorer. Même si une partie des entités assujetties s'efforce de mettre en place des dispositifs de lutte les plus efficaces possible, le manque de ressources, de moyens matériels, de formations et de coordination au niveau des autorités judiciaires qui traitent les dossiers en matière de blanchiment et de financement du terrorisme limite la portée de ces actions. Malgré un arsenal législatif reconnu comme efficace par les experts, la Belgique doit se donner les moyens de remédier aux manquements actuels de son dispositif de LBC/FT pour créer ainsi un système effectif performant.

Pour répondre à ces enjeux, plusieurs améliorations doivent être mises en œuvre au sein du dispositif de LBC/FT en Belgique où une mobilisation de l'ensemble des acteurs, tous interdépendants, est primordiale pour augmenter l'efficacité générale du système de lutte. Au niveau du législateur, de nouvelles améliorations du dispositif juridique devraient apparaître avec la transposition en droit national de la 5ème Directive *AML*, initialement prévue pour le 10 janvier 2020. Par une approche encore plus proactive et un renforcement de leur encadrement, les autorités de contrôle pourraient atténuer les lacunes actuelles constatées dans les dispositifs des entités assujetties qui, quant à elles, devraient procéder à une actualisation de leur évaluation globale des risques. De la part de la CTIF, l'amélioration de ses processus de communication avec la population, les entités assujetties et les déclarants renforcerait

leur compréhension dans la détection et la déclaration des opérations suspectes. Une amélioration importante est également attendue au niveau des autorités judiciaires puisqu'actuellement, elles n'ont pas les moyens nécessaires pour mener à bien leur devoir d'enquête ce qui impacte ainsi toute l'efficacité du dispositif de lutte. Le manque de ressources financières mises à disposition par le gouvernement est, aujourd'hui, un frein considérable dans la LBC/FT en Belgique

L'étude étant limitée à la Belgique et axée sur les institutions financières, il serait intéressant d'approfondir l'analyse de la mise en place de l'évaluation globale au niveau de l'ensemble des entités assujetties mais également de comparer comment l'approche fondée sur les risques est appliquée dans d'autres pays. Au vu du caractère transnational de cette lutte, cela permettrait une meilleure compréhension de la problématique et servirait ainsi à améliorer l'efficacité des dispositifs actuels et la coopération internationale.

Nous voudrions clôturer ce travail en soulignant la difficulté pour l'ensemble des acteurs de maintenir un combat à armes égales dans un domaine tel que la lutte contre le blanchiment des capitaux et le financement du terrorisme. En effet, entre l'augmentation des actes terroristes en Belgique et le développement de réseaux de blanchiment professionnels de plus en plus spécialisés, renouvelant constamment leurs techniques de fraude et exploitant les nouvelles possibilités offertes par la mondialisation, le travail du législateur se complexifie et le temps de réaction des acteurs de la lutte devient un élément déterminant pour assurer un système effectif efficace.

Il semble également qu'une prise de conscience de la part de la population mais surtout des autorités politiques belges sur l'importance des effets engendrés par le blanchiment et le financement du terrorisme est plus que nécessaire pour combattre au mieux ces deux phénomènes et limiter au plus vite leur impact sur notre société actuelle.

BIBLIOGRAPHIE

Ouvrages et articles scientifiques

ANDERSON, D. J., et EUBANKS, G. (2015), *Leveraging COSO across the Three Lines of Defense – The Institute of Internal Auditors*, Committee of Sponsoring Organizations of the Treadway Commission

BAUDRIHAYE-GÉRARD, L., et CARDON, M.-C. (2018), "La cellule de traitement des informations financières belge face au blanchiment (Ctif) : de l'emprise des flux aux ajustements du cadre", *Les arbitres de l'illégalisme : nouveau regard sur les manières de faire du contrôle social*, *C*hamp pénal, Vol. XV

BENRAAD, M. (2015), "Défaire Daech : une guerre tant financière que militaire", *Institut français des relations internationales*, 2015/2 Été, pp. 125-135

BERDEN, P. (2014), "De l'opération atypique à l'opération suspecte", dans CLESSE, C.-H., et NAGELS, C. (Éds.), *Vingt ans de lutte anti-blanchiment en Belgique – Bilan et perspectives*, pp.101-115, Bruylant, Bruxelles

BRAUX, C. (2015), *Analyse de la conformité et de l'efficacité du système belge de lutte contre le blanchiment de capitaux et le financement du terrorisme depuis 2005 : évolutions*, Mémoire de Master en Ingénieur de Gestion, Université de Namur, Namur

CHAPPEZ, J. (2003) "La lutte internationale contre le blanchiment des capitaux d'origine illicite et le financement du terrorisme", *Annuaire français de droit international*, Volume 49, pp. 542-562

COMISSION EUROPEENNE (2013), Proposition de Directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, Strasbourg

COMISSION EUROPEENNE (2019), Rapport de la Commission au Parlement européen et au Conseil sur l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme pesant sur le marché intérieur et liés aux activités transfrontières, Bruxelles

CTIF (2013), *Le livre blanc de l'argent noir – 20 ans de lutte contre le blanchiment et le financement du terrorisme*, Bruxelles

CTIF (2015a), *22ème Rapport d'activités 2015*, Bruxelles

CTIF (2015b), *22ème Rapport d'activités 2015 – Annexe 1 : Tendances de blanchiment et de financement du terrorisme*, Bruxelles

CTIF (2015c), *22ème Rapport d'activités 2015 – Annexe 2 : Statistiques*, Bruxelles

CTIF (2016), *23ème Rapport d'activités 2016*, Bruxelles

CTIF (2017), *24ème Rapport d'activités 2017*, Bruxelles

CTIF (2018), *25ème Rapport d'activités 2018*, Bruxelles

DAPSENS D'YVOIR, Y. (2016), *L'efficacité, la complémentarité et la réactivité des moyens de lutte contre le blanchiment des capitaux et le financement du terrorisme*, Mémoire de Master en Ingénieur de Gestion, Université de Namur, Namur

DEBRUYNE, G. (2019), *Le de-risking : origines et impact sur l'accès au monde financier des diamantaires belges*, Mémoire de Master en Sciences de Gestion, Université de Namur, Namur

DESSART, F. et STEILS, N. (2016), Études de marchés, Année académique 2016-2017, Université de Namur, Namur

DUFOUR, C. (2019), Méthodes de recherche en sciences de l'information, Année académique 2018-2019, Université de Montréal, Montréal

FABRI, C. (2016), *La transposition de la 4ème directive européenne relative à la lutte contre le blanchiment : Une opportunité pour la Belgique de mieux se conformer aux recommandations du Gafi ?*, Mémoire de Master en Sciences de Gestion, Université de Namur, Namur

FORIR, F. (2018), *Application de la loi anti-blanchiment par les réviseurs en Belgique : bilan et perspectives*, Mémoire de Master en Sciences de Gestion, HEC- Ecole de gestion de l'Université de Liège, Liège

FATF-GAFI (2012), *Recommandations du GAFI - Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération*, mise à jour octobre 2018, Paris

FATF-GAFI (2015a), *Emerging Terrorist Financing Risks*, Paris

FATF-GAFI (2015b), *Mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme en Belgique*, Rapport du quatrième cycle d'évaluations mutuelles, Paris

FATF-GAFI (2014), *Risk-Based Approach guidance for the banking sector*, Paris

FATF-GAFI (2018), *Mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme en Belgique*, 3ème Rapport de suivi renforcé & réévaluation de notations de conformité technique, Paris

GATOT, L. (2019), *Comment donner une assurance raisonnable quant à la réalisation des objectifs de lutte contre le blanchiment des capitaux ?*, IFE Séminaire «Lutte contre le blanchiment - Compliance», Bruxelles

HANE, T. (2015), *L'intelligence économique au service de la lutte contre le blanchiment de capitaux et le financement du terrorisme*, Thèse de Doctorat en Droit privé et sciences criminelles, Université de Strasbourg, Strasbourg

KOPP, P. (2006), "La lutte contre le blanchiment", dans FRISON-ROCHE, M.-A. (Éd.) *Les banques entre droit et économie*, LGDJ, Droit et Économie, p.33-47

KOUTOUZIS, M., et THONY, J.-F. (2005), *Le blanchiment*, Presses Universitaires de France, Paris

MAHAMOUD, I. (2014), "Comprendre le fonctionnement des hawalas : pour une meilleure régulation", *Épargne sans frontière*, N°114, pp. 45-54

NÉLIS, N. (2017), *« Risk based approach » dans la lutte contre le blanchiment des capitaux*, Mémoire de Master en Sciences de Gestion, Université de Namur, Namur

PEREIRA, B. (2011) "Blanchiment, soupçon et sécurité financière", *Revue Internationale de Droit Économique*, pp. 43-73

PWC (2018), "Pulling fraud out of the shadows", *Global Economic Crime and Fraud Survey 2018*

SCHNEIDER, F., et WINDISCHBAUER, U. (2010), "Money Laundering: Some Facts", *Economics of Security Working Paper*, 25, Berlin, pp.2-4

TAUZIN, P. (2014), "La gouvernance bancaire dans la lutte contre le blanchiment de capitaux", *Revue Internationale d'Intelligence Économique*, Lavoisier, Vol.6, pp.37-49

THE INSTITUTE OF INTERNAL AUDITORS (2013), *The Three Lines of Defense in Effective Risk Management and Control*, IAA Position Paper, p.2

TRACFIN (2015), "Les modes de financement du terrorisme et l'action des autorités publiques", *Rapport Moral Sur L'argent Dans Le Monde 2015-2016*, pp.295-301

TRACFIN (2018), *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017-2018*, Montreuil

VAN COILE, B. et VANDERSTICHELEN, B. (2015), "L'approche par les risques, nerf de la guerre contre le blanchiment de capitaux et le financement du terrorisme ! ", *Accountancy & Tax*, 2015/3, pp.4-63

VERHAGE, A. (2014), "Les pierres d'achoppement de la conformité LBC ", dans CLESSE, C.-H., et NAGELS, C. (Eds.), *Vingt ans de lutte anti-blanchiment en Belgique – Bilan et perspectives*, pp.117-147, Bruxelles : Bruylant

Sites internet et articles en ligne

ALCARAZ, M. (2007), "11 septembre 2001 : des volumes inhabituels sur les options peu avant l'attentat", *Les Echos*, consulté sur https://www.lesechos.fr/2007/09/11-septembre-2001-des-volumes-inhabituels-sur-les-options-peu-avant-lattentat-539426 le 3 décembre 2019

AUBRY, B. (2019), "Machine Learning : une arme efficace contre le blanchiment d'argent et le financement du terrorisme", *D.Views*, consulté sur https://blog.deloitte.fr/machine-learning-une-arme-efficace-contre-le-blanchiment-d-argent-et-le-financement-du-terrorisme/ le 4 janvier 2020

BANQUE MONDIALE (2019), *Le Groupe de la Banque mondiale et le Fonds monétaire international FMI*, Site internet officiel de la Banque Mondiale, consulté sur https://www.banquemondiale.org/fr/about/history/the-world-bank-group-and-the-imf le 9 décembre 2019

BLOOMENTHAL, A. (2019), "Dark Web", *Investopedia*, consulté sur https://www.investopedia.com/terms/d/dark-web.asp le 25 décembre 2019

BNB (2019), *Prévention du blanchiment de capitaux et du financement du terrorisme*, Site internet officiel de la Banque Nationale de Belgique, consulté sur https://www.nbb.be/fr/supervision-financiere/prevention-du-blanchiment-de-capitaux-et-du-financement-du-terrorisme le 15 décembre 2019

BNB & CTIF (2019), *Présentation de la séance d'information AML annuelle*, Site internet officiel de la CTIF, consulté sur https://www.nbb.be/doc/ts/enterprise/conferences/20191106_aml_infosession.pdf le 5 janvier 2020

BOLUZE, L. (2019), "Crowdfunding : définition et fonctionnement", *Capital*, consulté sur https://www.capital.fr/economie-politique/crowdfunding-1316742 le 25 décembre 2019

BOUTRY, T., et DÉCUGIS, J.-M. (2018), "Lutte contre le financement de Daech : «L'argent permet d'identifier des terroristes» ", *Le Parisien*, consulté sur https://www.leparisien.fr/faits-divers/lutte-contre-le-financement-de-daech-l-argent-permet-d-identifier-des-terroristes-25-04-2018-7683828.php le 4 décembre 2019

BUYLE, J.-P., et CLOQUET, L. (2016), "Les banques face au de-risking, un exercice de funambule", *L'Echo,* consulté sur https://www.lecho.be/opinions/analyse/les-banques-face-au-de-risking-un-exercice-de-funambule/9786257.html le 3 janvier 2020

COE (2019), *Cellules de renseignement financier*, Portail du Conseil de l'Europe, consulté sur https://www.coe.int/fr/web/moneyval/implementation/fiu le 9 décembre

CTIF (2019), Site internet officiel de la Cellule de Traitement des Informations Financières, consulté sur http://www.ctif-cfi.be/website/

DE BONY, C.-H. (2019), "L'intelligence artificielle dans le KYC : quels bénéfices pour les Assets Managers ?", *Revue Banque*, n°803, consulté sur http://www.revue-banque.fr/management-fonctions-supports/article/intelligence-artificielle-dans-kyc-quels-benefices#desc-puce-nbp-1 le 4 janvier 2020

DEMPURÉ, F. (2017) "La fraude au président", *Les Échos*, consulté sur https://business.lesechos.fr/entrepreneurs/juridique/dossiers/11622811/tpepme-00011622811-1-la-fraude-au-president-317046.php le 5 janvier 2020

EGMONT GROUP (2019), *About Egmont group*, Site internet officiel du groupe Egmont, consulté sur https://www.egmontgroup.org/fr/content/about-fr le 9 décembre 2019

EUROPA (2019), *Règlements, directives et autres actes législatifs*, Site internet officiel de l'Union Européenne, consulté sur https://europa.eu/european-union/abouteuropa_fr le 9 décembre 2019

FATF-GAFI (2019a), *Foire aux questions*, Site internet officiel du GAFI, Consulté sur https://www.fatf-gafi.org/fr/foireauxquestionsfaq/blanchimentdecapitaux/#d.fr.11223 le 28 novembre 2019

FATF-GAFI (2019b), *A propos du GAFI*, Site internet officiel du GAFI, consulté sur https://www.fatf-gafi.org/fr/aproposdugafi/ le 7 décembre 2019

FATF-GAFI (2019c), *Pays*, Site internet officiel du GAFI, consulté sur https://www.fatf-gafi.org/fr/pays/ le 7 décembre 2019

FEBELFIN (2019), *PSD2 : liste des questions les plus fréquemment posées,* Site internet de Febelfin, consulté sur https://www.febelfin.be/fr/consommateurs/article/psd2-liste-des-questions-les-plus-frequemment-posees le 26 décembre 2019

JOUVET, F. (2018), "Comment fonctionnait l'Etat islamique?", *L'Écho,* Consulté sur https://www.lecho.be/economie-politique/international/asie/comment-fonctionnait-l-etat-islamique/9999451.html le 3 décembre 2019

MEES, K. (2017), "La nouvelle Loi anti-blanchiment est parue au Moniteur", *Polinfo*, consulté sur https://polinfo.kluwer.be/newsview.aspx?contentdomains=POLINFO&id=VS300559563_&lang=fr le 10 décembre 2019

OCDE (2019a), *Découvrez l'OCDE*, Site internet officiel du Conseil de l'Europe, consulté sur http://www.oecd.org/fr/general/Informations-cles-sur-OCDE.pdf le 8 décembre 2019

OCDE (2019b), *Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme : diminution des risques*, Site internet officiel du Conseil de l'Europe, consulté sur https://www.coe.int/fr/web/moneyval/implementation/de-risking le 3 janvier 2020

ONU (2019), *À propos de l'ONU*, Site internet officiel de l'Organisation des Nations Unies, consulté sur https://www.un.org/fr/about-un/index.html le 9 décembre 2019

PAIANO, J. (2018), "Comprendre les crypto-monnaies en 10 minutes", *Trust my science*, consulté sur https://trustmyscience.com/comprendre-les-crypto-monnaies-en-10-minutes/ le 12 décembre 2019

RTBF (2018), *Corruption internationale: "Les mafias se sont substituées aux banques" dénonce le juge Claise*, Site internet de la RTBF, consulté sur https://www.rtbf.be/info/societe/detail_corruption-internationale-une-atteinte-aux-nations-democratiques?id=10025916 le 5 janvier 2020

SPF ECONOMIE (2019), *Lutte contre le blanchiment de capitaux et le financement du terrorisme*, Site internet officiel du Service public fédéral Économie, consulté sur https://economie.fgov.be/fr/themes/services-financiers/lutte-contre-le-blanchiment-de le 25 novembre 2019

TREFFEL, R. (2015), "Le délit d'initié du 11 Septembre 2001", *L'économiste*, consulté sur https://www.leconomiste.eu/decryptage-economie/366-le-delit-d-initie-du-11-septembre-2001.html le 3 décembre 2019

UNODC (2018), *Money-laundering*, Site internet officiel de l'Office des Nations Unies contre la drogue et le crime, consulté sur https://www.unodc.org/e4j/en/organized-crime/module-4/key-issues/money-laundering.html le 24 novembre 2019

UNODC (2019a), *UN Instruments and Other Relevant International Standards on Money-Laundering and Terrorist Financing*, Site internet officiel de l'Office des Nations Unies contre la drogue et le crime, consulté sur https://www.unodc.org/unodc/en/money-laundering/Instruments-Standards.html?ref=menuside#UN-Conventions le 8 décembre 2019

UNODC (2019b), *Technical assistance against money-laundering*, Site internet officiel de l'Office des Nations Unies contre la drogue et le crime, consulté sur https://www.unodc.org/unodc/en/money-laundering/technical-assistance.html le 8 décembre 2019

VERNIER, E. (2017), "Blanchiment de capitaux : des techniques et des circuits plus complexes", *S&D Magazine*, consulté sur https://sd-magazine.com/avis-experts/blanchiment-de-capitaux-techniques-circuits-plus-complexes le 16 novembre 2019

Textes légaux

Circulaire n°2018_01 de la Banque Nationale de Belgique du 15 janvier 2018 relative à l'évaluation globale des risques en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, disponible sur https://www.nbb.be/fr

Circulaire n°2018_02 de la Banque Nationale de Belgique du 24 janvier 2018 relative au questionnaire périodique relatif à la prévention du blanchiment de capitaux et du financement du terrorisme, disponible sur https://www.nbb.be/fr

Circulaire n°2019_20 de la Banque Nationale de Belgique du 19 juillet 2019 relative aux attentes concernant les activités liées aux crypto-actifs, disponible sur https://www.nbb.be/fr

Directive 91/308/CEE du Conseil du 10 juin 1991 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux, *J.O.C.E.*, L 166, 28 juin 1991

Directive 2001/97/CE du Parlement européen et du Conseil du 4 décembre 2001 modifiant la directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux, *J.O.C.E.*, L 344, 28 décembre 2001

Directive 2005/60/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, *J.O.U.E.*, L 309, 25 novembre 2008

Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, *J.O.U.E.*, L 141, 5 juin 2015

Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE, *J.O.U.E.*, L 156, 19 juin 2018

Loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, *M.B.*, 9 février 1993

Loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse, *M.B.*, 7 mai 2014, *err.*, 21 mai 2019

Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, *M.B.*, 6 octobre 2017

Projet de loi relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, Exposé des motifs, *Doc.*, Ch., 2016-2017, 2566/001, pp.5-306

Résolution 49/60 de l'Assemblée générale des Nations Unies, A/RES/49/60 (1994), 17 février 1995

Résolution 2199 du Conseil de sécurité, S/RES/2199 (2015), 12 février 2015

ANNEXES

Annexe 1 : Les 40 recommandations du GAFI

LES RECOMMANDATIONS DU GAFI

A. POLITIQUES ET COORDINATION EN MATIÈRE DE LBC/FT

1. Évaluation des risques et application d'une approche fondée sur les risques *

Les pays devraient identifier, évaluer et comprendre les risques de blanchiment de capitaux et de financement du terrorisme auxquels ils sont exposés et devraient prendre des mesures, parmi lesquelles la désignation d'une autorité ou d'un mécanisme pour coordonner les actions d'évaluation des risques, et mobiliser des ressources, afin de s'assurer que les risques sont efficacement atténués. Sur la base de cette évaluation, les pays devraient appliquer une approche fondée sur les risques pour s'assurer que les mesures de prévention et d'atténuation du blanchiment de capitaux et du financement du terrorisme sont à la mesure des risques identifiés. Cette approche devrait constituer le fondement essentiel d'une allocation efficiente des ressources au sein du régime de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) et de la mise en œuvre de mesures fondées sur les risques pour toutes les recommandations du GAFI. Lorsque les pays identifient des risques plus élevés, ils devraient s'assurer que leur régime de LBC/FT fait face à ces risques de manière satisfaisante. Lorsque les pays identifient des risques plus faibles, ils peuvent décider d'autoriser sous certaines conditions des mesures simplifiées pour certaines recommandations du GAFI.

Les pays devraient obliger les institutions financières et les entreprises et professions non financières désignées à identifier et évaluer leurs risques de blanchiment de capitaux et de financement du terrorisme et à prendre des mesures efficaces pour les atténuer.

2. Coopération et coordination nationales

Les pays devraient disposer de politiques nationales de LBC/FT prenant en compte les risques identifiés. Ces politiques devraient être régulièrement réexaminées. Les pays devraient désigner une autorité ou disposer d'un mécanisme de coordination ou de tout autre mécanisme responsable de ces politiques.

Les pays devraient s'assurer que les responsables de l'élaboration des politiques, la cellule de renseignements financiers (CRF), les autorités de poursuite pénale, les autorités de contrôle et les autres autorités compétentes concernées, tant au niveau opérationnel qu'à celui de l'élaboration des politiques, disposent de mécanismes efficaces leur permettant de coopérer et, le cas échéant, de se coordonner et d'échanger des informations au plan national pour l'élaboration et la mise en œuvre des politiques et des activités visant à lutter contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive. Cela devrait inclure la coopération et la coordination entre autorités compétentes pour assurer la compatibilité des exigences de LBC/FT avec les mesures de protection des données et du respect de la vie privée, et autres dispositions similaires (ex. sécurité et localisation des données).

B. BLANCHIMENT DE CAPITAUX ET CONFISCATION

3. Infraction de blanchiment de capitaux *

Les pays devraient conférer le caractère d'infraction pénale au blanchiment de capitaux sur la base de la Convention de Vienne et de la Convention de Palerme. Les pays devraient appliquer l'infraction de blanchiment de capitaux à toutes les infractions graves afin de couvrir la gamme la plus large d'infractions sous-jacentes.

4. Confiscation et mesures provisoires *

Les pays devraient adopter des mesures similaires à celles prévues par la Convention de Vienne, la Convention de Palerme et la Convention sur le financement du terrorisme, y compris des mesures législatives, afin de permettre à leurs autorités compétentes de geler ou saisir et de confisquer, sans préjudice des droits des tiers de bonne foi : (a) les biens blanchis ; (b) le produit de, ou les instruments utilisés pour le, ou destinés à être utilisés en vue du blanchiment de capitaux ou d'infractions sous-jacentes ; (c) les biens qui constituent le produit du, sont utilisés pour le, ou destinés à être utilisés en vue du ou affectés au financement du terrorisme, des actes terroristes ou des organisations terroristes ; et (d) des biens d'une valeur correspondante.

De telles mesures devraient comprendre le pouvoir : (a) d'identifier, de dépister et d'estimer les biens faisant l'objet d'une mesure de confiscation ; (b) de mettre en œuvre des mesures provisoires, telles que le gel et la saisie, afin de faire obstacle à toute opération sur ou tout transfert ou disposition de ces biens ; (c) de prendre des mesures pour empêcher ou annuler les actions qui compromettent la faculté du pays de geler, saisir ou recouvrer les biens faisant l'objet d'une mesure de confiscation ; et (d) de prendre toutes les mesures d'enquête appropriées.
Les pays devraient envisager d'adopter des mesures permettant la confiscation de tels produits ou instruments sans condamnation pénale préalable (confiscation sans condamnation préalable) ou des mesures obligeant l'auteur présumé de l'infraction à apporter la preuve de l'origine licite des biens présumés passibles de confiscation, dans la mesure où une telle obligation est conforme aux principes de leur droit interne.

C. FINANCEMENT DU TERRORISME ET FINANCEMENT DE LA PROLIFÉRATION

5. Infraction de financement du terrorisme *
Les pays devraient conférer le caractère d'infraction pénale au financement du terrorisme sur la base de la Convention sur le financement du terrorisme, et devraient conférer le caractère d'infraction pénale non seulement au financement des actes terroristes mais également au financement des organisations terroristes et des individus terroristes, y compris en l'absence de lien avec un ou plusieurs actes terroristes spécifiques. Les pays devraient s'assurer que de telles infractions sont des infractions sous-jacentes au blanchiment de capitaux.

6. Sanctions financières ciblées liées au terrorisme et au financement du terrorisme *
Les pays devraient mettre en œuvre des régimes de sanctions financières ciblées conformément aux résolutions du Conseil de sécurité des Nations Unies relatives à la prévention et la répression du terrorisme et du financement du terrorisme. Les résolutions obligent les pays à geler sans délai les fonds et autres biens de, et à s'assurer qu'aucun fonds ou autre bien ne soit mis, directement ou indirectement, à la disposition ou au profit de toute personne ou entité (i) désignée par le ou sous l'autorité du Conseil de sécurité des Nations Unies au titre du Chapitre VII de la Charte des Nations Unies, y compris en vertu de la résolution 1267 (1999) et de ses résolutions subséquentes ou (ii) désignée par ce pays conformément à la résolution 1373 (2001).

7. Sanctions financières ciblées liées à la prolifération *
Les pays devraient mettre en œuvre des sanctions financières ciblées conformément aux résolutions du Conseil de sécurité des Nations Unies relatives à la prévention, la répression et l'interruption de la prolifération des armes de destruction massive et de son financement. Ces résolutions obligent les pays à geler sans délai les fonds et autres biens de, et à s'assurer qu'aucun fonds ou autre bien ne soit mis, directement ou indirectement, à la disposition ou au profit de toute personne ou entité désignée par le ou sous l'autorité du Conseil de sécurité des Nations Unies au titre du Chapitre VII de la Charte des Nations Unies.

8. Organismes à but non lucratif *
Les pays devraient examiner la pertinence de leurs lois et règlements relatifs aux organismes à but non lucratif qu'ils ont identifiés comme vulnérables à une exploitation à des fins de financement du terrorisme. Les pays devraient appliquer des mesures ciblées et proportionnées à ces OBNL, selon une approche basée sur les risques, pour les protéger d'une exploitation à des fins de financement du terrorisme, commise notamment :
(a) par des organisations terroristes se présentant comme des entités légitimes ;
(b) en exploitant des entités légitimes comme moyens de financement du terrorisme, y compris pour éviter les mesures de gel des avoirs ;
(c) en dissimulant ou opacifiant le détournement clandestin de fonds destinés à des fins légitimes vers des organisations terroristes.

D. MESURES PRÉVENTIVES

9. Lois sur le secret professionnel des institutions financières
Les pays devraient s'assurer que les lois sur le secret professionnel des institutions financières n'entravent pas la mise en œuvre des recommandations du GAFI

DEVOIR DE VIGILANCE RELATIF À LA CLIENTÈLE ET CONSERVATION DES DOCUMENTS
10. Devoir de vigilance relatif à la clientèle *

Il devrait être interdit aux institutions financières de tenir des comptes anonymes et des comptes sous des noms manifestement fictifs.

Les institutions financières devraient être obligées de prendre des mesures de vigilance à l'égard de leur clientèle lorsque :

(i) elles établissent des relations d'affaires ;

(ii) elles effectuent des opérations occasionnelles (i) supérieures au seuil désigné applicable (15 000 USD/EUR) ou (ii) sous forme de virements électroniques dans les circonstances visées par la note interprétative de la recommandation 16 ;

(iii) il existe un soupçon de blanchiment de capitaux ou de financement du terrorisme ;

(iv) l'institution financière doute de la véracité ou de la pertinence des données d'identification du client précédemment obtenues.

Le principe selon lequel les institutions financières devraient exercer leur devoir de vigilance relatif à la clientèle devrait être prescrit par la loi. Chaque pays peut déterminer la façon dont il impose les obligations de vigilance spécifiques, soit par la loi, soit par des moyens contraignants.

Les mesures de vigilance relatives à la clientèle devant être prises sont les suivantes :

(a) Identifier le client et vérifier son identité au moyen de documents, données et informations de sources fiables et indépendantes.

(b) Identifier le bénéficiaire effectif et prendre des mesures raisonnables pour vérifier son identité de sorte que l'institution financière a l'assurance de savoir qui est le bénéficiaire effectif. Pour les personnes morales et les constructions juridiques, ceci devrait impliquer que les institutions financières comprennent la structure de propriété et de contrôle du client.

(c) Comprendre et, le cas échéant, obtenir des informations sur l'objet et la nature envisagée de la relation d'affaires.

(d) Exercer une vigilance constante à l'égard de la relation d'affaires et assurer un examen attentif des opérations effectuées pendant toute la durée de cette relation d'affaires, afin de s'assurer qu'elles sont cohérentes avec la connaissance qu'a l'institution financière de son client et des activités commerciales et du profil de risque de ce client, ce qui comprend, le cas échéant, l'origine des fonds.

Les institutions financières devraient être obligées d'appliquer chacune des mesures de vigilance indiquées aux points (a) à (d) ci-dessus mais devraient déterminer l'étendue de ces mesures en se fondant sur l'approche fondée sur les risques conformément aux notes interprétatives de la présente recommandation et de la recommandation 1.

Les institutions financières devraient être obligées de vérifier l'identité du client et du bénéficiaire effectif avant ou pendant l'établissement d'une relation d'affaires ou la réalisation des opérations dans le cas de clients occasionnels. Les pays peuvent autoriser les institutions financières à achever ces vérifications dès que cela est raisonnablement possible après l'établissement de la relation, dès lors que les risques de blanchiment de capitaux et de financement du terrorisme sont efficacement gérés et qu'il est essentiel de ne pas interrompre le déroulement normal des affaires.

Lorsque l'institution financière ne peut pas respecter les obligations des points (a) à (d) ci-dessus (dont l'étendue est modulée de façon appropriée en fonction de l'approche fondée sur les risques), elle devrait avoir l'obligation de ne pas ouvrir le compte, de ne pas établir la relation d'affaires ou de ne pas effectuer l'opération ; ou devrait être obligée de mettre un terme à la relation d'affaires ; et devrait envisager de faire une déclaration d'opération suspecte concernant le client.

Ces obligations devraient s'appliquer à tous les nouveaux clients, mais les institutions financières devraient également appliquer la présente recommandation aux clients existants, selon leur importance relative et les risques qu'ils représentent, et devraient exercer leur devoir de vigilance vis-à-vis de ces relations existantes en temps opportun.

11. Conservation des documents

Les institutions financières devraient être obligées de conserver, pendant au moins cinq ans, tous les documents nécessaires relatifs aux opérations, nationales et internationales, afin de leur permettre de répondre rapidement aux demandes d'information des autorités compétentes. Ces documents doivent être suffisants pour permettre la reconstitution d'opérations particulières (y compris les montants et, le cas échéant, les devises en cause) afin de fournir, si nécessaire, des preuves dans le cadre de poursuites relatives à une activité criminelle.

Les institutions financières devraient être obligées de conserver tous les documents obtenus dans le cadre des mesures de vigilance relatives à la clientèle (par exemple, la copie des documents officiels d'identification tels que les passeports, les cartes d'identité, les permis de conduire ou d'autres documents similaires, ou les informations figurant dans ces documents), les livres de comptes et la correspondance commerciale, y compris les résultats de toute analyse réalisée (par exemple, les recherches visant à établir le contexte et l'objet des opérations complexes d'un montant anormalement élevé) pendant au moins cinq ans à compter de la fin de la relation d'affaires ou de la date de l'opération occasionnelle.

Les institutions financières devraient être obligées par la loi de conserver les documents sur les opérations et les informations obtenues dans le cadre des mesures de vigilance relatives à la clientèle.

Les informations obtenues dans le cadre des mesures de vigilance relatives à la clientèle et les documents relatifs aux opérations devraient être mis à disposition des autorités compétentes nationales lorsque ces dernières en ont le pouvoir.

MESURES SUPPLÉMENTAIRES DANS LE CAS DE CLIENTS ET D'ACTIVITÉS SPÉCIFIQUES

12. Personnes politiquement exposées *

A l'égard des personnes politiquement exposées (PPE) étrangères (qu'elles soient des clients ou des bénéficiaires effectifs), les institutions financières devraient être obligées, en plus des mesures de vigilance normales relatives à la clientèle, de :

(a) disposer de systèmes appropriés de gestion des risques permettant de déterminer si le client ou le bénéficiaire effectif est une personne politiquement exposée ;
(b) obtenir l'autorisation de la haute direction d'établir (ou de poursuivre, s'il s'agit d'un client existant) de telles relations d'affaires ;
(c) prendre des mesures raisonnables pour établir l'origine du patrimoine et l'origine des fonds ;
(d) assurer une surveillance continue renforcée à l'égard de la relation d'affaires.

Les institutions financières devraient être obligées de prendre des mesures raisonnables pour déterminer si un client ou bénéficiaire effectif est une PPE nationale ou une personne qui exerce ou a exercé une fonction importante au sein de ou pour le compte d'une organisation internationale. Lorsque les relations d'affaires avec de telles personnes présentent un risque plus élevé, les institutions financières devraient être obligées d'appliquer les mesures des points (b), (c) et (d).

Les obligations applicables à tous les types de PPE devraient également s'appliquer aux membres de la famille de ces PPE et aux personnes qui leur sont étroitement associées.

13. Correspondance bancaire *

En ce qui concerne les relations de correspondance bancaire transfrontalière et les autres relations similaires, les institutions financières devraient être obligées, en plus des mesures de vigilance normales relatives à la clientèle, de :

(a) rassembler suffisamment d'informations sur le correspondant afin de pleinement comprendre la nature de ses activités et d'évaluer, sur la base d'informations publiquement disponibles, sa réputation et la qualité du contrôle dont il est l'objet, ce qui implique notamment de savoir si le correspondant a fait l'objet d'une enquête ou de mesures de la part d'une autorité de contrôle en matière de blanchiment de capitaux ou de financement du terrorisme ;
(b) évaluer les contrôles mis en place par le correspondant en matière de LBC/FT ;
(c) obtenir l'autorisation de la haute direction avant d'établir de nouvelles relations de correspondance bancaire ;
(d) comprendre clairement les responsabilités respectives de chaque institution ;
(e) en ce qui concerne les comptes de passage, avoir l'assurance que le correspondant a appliqué des mesures de vigilance aux clients ayant un accès direct aux comptes de la banque correspondante et qu'il est en mesure de fournir les informations pertinentes s'y rapportant sur demande de la banque correspondante.

Il devrait être interdit aux institutions financières d'établir ou de poursuivre une relation de correspondance bancaire avec des banques fictives. Les institutions financières devraient être obligées de s'assurer que les correspondants n'autorisent pas les banques fictives à utiliser leurs comptes.

14. Services de transfert de fonds ou de valeurs *

Les pays devraient prendre des mesures afin de s'assurer que les personnes physiques ou morales qui fournissent des services de transfert de fonds ou de valeurs sont agréées ou enregistrées et qu'elles font l'objet de systèmes efficaces de surveillance garantissant qu'elles respectent les obligations applicables découlant des recommandations du GAFI. Les pays devraient prendre des mesures afin d'identifier les personnes physiques ou morales qui fournissent des services de transfert de fonds ou de valeurs sans être agréées ou enregistrées, afin de leur appliquer des sanctions appropriées.

Toute personne physique ou morale qui opère en tant qu'agent devrait également être agréée ou enregistrée par une autorité compétente, ou le prestataire de services de transfert de fonds ou de valeurs devrait tenir à jour une liste de ses agents accessible aux autorités compétentes des pays dans lesquels le prestataire de services de transfert de fonds ou de valeurs et ses agents opèrent. Les pays devraient prendre des mesures afin de s'assurer que les prestataires de services de transfert de fonds ou de valeurs recourant à des agents les intègrent dans leurs programmes de LBC/FT et surveillent le respect par ces agents de ces programmes.

15. Nouvelles technologies

Les pays et les institutions financières devraient identifier et évaluer les risques de blanchiment de capitaux ou de financement du terrorisme pouvant résulter (a) du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris de nouveaux mécanismes de distribution, et (b) de l'utilisation de technologies nouvelles ou en développement en lien avec

de nouveaux produits ou des produits préexistants. Dans le cas des institutions financières, cette évaluation du risque devrait avoir lieu avant le lancement des nouveaux produits ou des nouvelles pratiques commerciales ou avant l'utilisation de technologies nouvelles ou en développement. Les institutions financières devraient prendre les mesures appropriées pour gérer et atténuer ces risques.

Pour gérer et atténuer les risques émergeant d'actifs virtuels, les pays devraient s'assurer que les prestataires de services liés à des actifs virtuels sont réglementés à des fins de LBC/FT, et agréés ou enregistrés, et soumis à des systèmes efficaces de surveillance garantissant qu'ils respectent les obligations applicables découlant des Recommandations du GAFI.

16. Virements électroniques *

Les pays devraient s'assurer que les institutions financières incluent les informations requises et exactes sur le donneur d'ordre ainsi que les informations requises sur le bénéficiaire dans les virements électroniques et autres messages qui s'y rapportent, et que ces informations accompagnent le virement électronique ou le message qui s'y rapporte tout au long de la chaîne de paiement.

Les pays devraient s'assurer que les institutions financières surveillent les virements électroniques afin de détecter ceux qui ne comportent pas les informations requises sur le donneur d'ordre et/ou le bénéficiaire et qu'elles prennent les mesures appropriées.

Les pays devraient s'assurer que, dans le cadre du traitement des virements électroniques, les institutions financières prennent des mesures de gel et devraient interdire la conduite d'opérations avec les personnes et entités désignées, conformément aux obligations des résolutions du Conseil de sécurité des Nations Unies pertinentes, telles que la résolution 1267 (1999) et les résolutions ultérieures et la résolution 1373 (2001), relatives à la prévention et la répression du terrorisme et du financement du terrorisme.

RECOURS À DES TIERS, CONTRÔLES ET GROUPES FINANCIERS

17. Recours à des tiers *

Les pays peuvent autoriser les institutions financières à recourir à des tiers pour s'acquitter des points (a) à (c) des mesures de vigilance relatives à la clientèle prévues dans la recommandation 10 ou pour jouer le rôle d'apporteur d'affaires, à condition que les critères précisés ci-dessous soient respectés. Lorsqu'un tel recours est autorisé, la responsabilité finale de la mise en œuvre des mesures de vigilance relatives à la clientèle reste celle de l'institution financière ayant eu recours au tiers.

Les critères qui devraient être respectés sont les suivants :

Une institution financière ayant recours à un tiers devrait obtenir immédiatement les informations nécessaires concernant les points (a) à (c) des mesures de vigilance relatives à la clientèle prévues dans la recommandation 10.

Les institutions financières devraient prendre les mesures appropriées pour avoir l'assurance que le tiers est à même de fournir, sur demande et sans délai, la copie des données d'identification et autres documents pertinents liés au devoir de vigilance relatif à la clientèle.

L'institution financière devrait avoir l'assurance que le tiers est soumis à une réglementation, qu'il fait l'objet d'un contrôle ou d'une surveillance et qu'il a pris des mesures pour respecter les obligations de vigilance relatives à la clientèle et les obligations de conservation des documents, conformément aux recommandations 10 et 11.

Les pays devraient tenir compte des informations disponibles sur le niveau de risque lié aux pays lorsqu'ils décident des pays dans lesquels les tiers satisfaisant les critères peuvent être établis.

Lorsqu'une institution financière a recours à un tiers faisant partie du même groupe financier et (i) lorsque ce groupe met en œuvre, d'une part, les obligations de vigilance relatives à la clientèle et de conservation des documents conformément aux recommandations 10, 11 et 12 et, d'autre part, des programmes de LBC/FT conformément à la recommandation 18 ; et (ii) lorsque la mise en œuvre efficace de ces obligations de vigilance et de conservation des documents et des programmes de LBC/FT est contrôlée au niveau du groupe par une autorité compétente, alors les autorités compétentes pertinentes peuvent considérer que l'institution financière applique les mesures prévues aux points (b) et (c) ci-dessus au moyen du programme du groupe, et peuvent décider que le point (d) n'est pas une condition préalable nécessaire au recours à un tiers lorsque le risque plus élevé présenté par le pays est atténué de manière satisfaisante par les politiques de LBC/FT du groupe.

18. Contrôles internes et succursales et filiales à l'étranger *

Les institutions financières devraient être obligées de mettre en œuvre des programmes de LBC/FT. Les groupes financiers devraient être obligés de mettre en œuvre des programmes de LBC/FT à l'échelle du groupe, y compris des politiques et procédures de partage des informations au sein du groupe aux fins de LBC/FT.

Les institutions financières devraient être obligées de s'assurer que leurs succursales et filiales majoritaires à l'étranger appliquent, au moyen des programmes du groupe financier contre le blanchiment de capitaux et le financement du terrorisme, des mesures de LBC/FT conformes aux obligations du pays d'origine mettant en œuvre les recommandations du GAFI.

19. Pays présentant un risque plus élevé *

Les institutions financières devraient être obligées d'appliquer des mesures de vigilance renforcées aux relations d'affaires et opérations avec les personnes, physiques ou morales, ainsi qu'avec les institutions financières, des pays pour lesquels le GAFI appelle à le faire. Le type de mesures de vigilance renforcées appliquées devrait être efficace et proportionnel aux risques.

Les pays devraient être en mesure d'appliquer des contre-mesures adaptées lorsque le GAFI les appelle à le faire. Les pays devraient également être à même d'appliquer des contremesures indépendamment de tout appel du GAFI. Ces contre-mesures devraient être efficaces et proportionnelles aux risques.

DÉCLARATION DES OPÉRATIONS SUSPECTES

20. Déclaration des opérations suspectes *

Lorsqu'une institution financière suspecte, ou a des motifs raisonnables de suspecter, que des fonds sont le produit d'une activité criminelle ou ont un rapport avec le financement du terrorisme, elle devrait être obligée en vertu de la loi de faire immédiatement une déclaration d'opération suspecte à la cellule de renseignements financiers (CRF).

21. Divulgation et confidentialité

Les institutions financières, leurs dirigeants et employés devraient être :

(a) protégés par la loi contre toute responsabilité pénale ou civile pour violation de toute règle encadrant la divulgation d'informations imposée par contrat ou par toute disposition législative, réglementaire ou administrative, lorsqu'ils déclarent de bonne foi leurs soupçons à la CRF, même s'ils ne savaient pas précisément quelle était l'activité criminelle sous-jacente ou si l'activité illégale ayant fait l'objet du soupçon ne s'est pas effectivement produite ;

(b) soumis à une interdiction par la loi de divulguer le fait qu'une déclaration d'opération suspecte (DOS) ou une information s'y rapportant est communiquée à la CRF. Ces dispositions ne visent pas à entraver le partage d'informations prévu par la Recommandation 18.

ENTREPRISES ET PROFESSIONS NON FINANCIÈRES

22. Entreprises et professions non financières désignées – Devoir de vigilance relatif à la clientèle *

Les obligations de vigilance relatives à la clientèle et de conservation des documents prévues par les recommandations 10, 11, 12, 15 et 17 s'appliquent aux entreprises et professions non financières désignées dans les situations suivantes :

(a) Casinos – lorsque les clients effectuent des opérations financières égales ou supérieures au seuil désigné applicable.

(b) Agents immobiliers – lorsqu'ils sont impliqués dans des transactions pour leurs clients concernant l'achat ou la vente de biens immobiliers.

(c) Négociants en métaux précieux et négociants en pierres précieuses – lorsqu'ils effectuent avec un client une opération en espèces égale ou supérieure au seuil désigné applicable.

(d) Avocats, notaires, autres professions juridiques indépendantes et comptables – lorsqu'ils préparent ou effectuent des transactions pour leurs clients concernant les activités suivantes :
- achat et vente de biens immobiliers ;
- gestion de capitaux, de titres ou autres actifs du client ;
- gestion de comptes bancaires, d'épargne ou de titres ;
- organisation des apports pour la création, l'exploitation ou la gestion de sociétés ;
- création, exploitation ou administration de personnes morales ou de constructions juridiques, et achat et vente d'entités commerciales.

(e) Prestataires de services aux trusts et aux sociétés – lorsqu'ils préparent ou effectuent des opérations pour un client en lien avec les activités suivantes :
- ils agissent en qualité d'agent pour la constitution de personnes morales ;
- ils agissent (ou ils prennent des mesures afin qu'une autre personne agisse) en qualité de dirigeant ou de secrétaire général (secretary) d'une société de capitaux, d'associé d'une société de personnes ou de titulaire d'une fonction similaire pour d'autres types de personnes morales ;
- ils fournissent un siège social, une adresse commerciale ou des locaux, une adresse administrative ou postale à une société de capitaux, une société de personnes ou toute autre personne morale ou construction juridique ;

- ils agissent (ou ils prennent des mesures afin qu'une autre personne agisse) en qualité de trustee d'un trust exprès ou exercent une fonction équivalente pour une autre forme de construction juridique ;
- ils agissent (ou ils prennent des mesures afin qu'une autre personne agisse) en qualité d'actionnaire agissant pour le compte d'une autre personne (nominee shareholder).

23. Entreprises et professions non financières désignées – Autres mesures *

Les obligations des recommandations 18 à 21 s'appliquent à toutes les entreprises et professions non financières désignées, dans les circonstances suivantes :

(a) Les avocats, les notaires, les autres professions juridiques indépendantes et les comptables devraient être obligés de déclarer les opérations suspectes lorsque, au nom ou pour le compte d'un client, ils effectuent une opération financière en lien avec les activités décrites au point (d) de la recommandation 22. Les pays sont vivement encouragés à étendre l'obligation de déclaration aux autres activités professionnelles exercées par les comptables, en particulier l'activité de vérification des comptes.

(b) Les négociants en métaux précieux et les négociants en pierres précieuses devraient être obligés de déclarer les opérations suspectes lorsqu'ils effectuent avec un client des opérations en espèces égales ou supérieures au seuil désigné applicable.

(c) Les prestataires de services aux trusts et aux sociétés devraient être obligés de déclarer les opérations suspectes lorsque, au nom ou pour le compte d'un client, ils effectuent une opération en lien avec les activités visées au point (e) de la recommandation 22.

E. TRANSPARENCE ET BÉNÉFICIAIRES EFFECTIFS DES PERSONNES MORALES ET CONSTRUCTIONS JURIDIQUES

24. Transparence et bénéficiaires effectifs des personnes morales *

Les pays devraient prendre des mesures pour empêcher l'utilisation des personnes morales à des fins de blanchiment de capitaux ou de financement du terrorisme. Les pays devraient s'assurer que des informations satisfaisantes, exactes et à jour sur les bénéficiaires effectifs et sur le contrôle des personnes morales peuvent être obtenues ou sont accessibles en temps opportun par les autorités compétentes. En particulier, les pays dans lesquels les personnes morales peuvent émettre des actions au porteur ou des bons de souscription d'actions au porteur, ou qui autorisent les actionnaires ou administrateurs agissant pour le compte d'une autre personne (nominee shareholders or nominee directors), devraient prendre des mesures efficaces pour s'assurer qu'elles ne sont pas détournées à des fins de blanchiment de capitaux ou de financement du terrorisme. Les pays devraient envisager de prendre des mesures pour faciliter l'accès aux informations sur les bénéficiaires effectifs et sur le contrôle des personnes morales par les institutions financières et les entreprises et professions non financières désignées lorsqu'elles mettent en œuvre les obligations des recommandations 10 et 22.

25. Transparence et bénéficiaires effectifs des constructions juridiques *

Les pays devraient prendre des mesures pour empêcher l'utilisation des constructions juridiques à des fins de blanchiment de capitaux ou de financement du terrorisme. En particulier, les pays devraient s'assurer que des informations satisfaisantes, exactes et à jour sur les trusts exprès, parmi lesquelles des informations sur le constituant, le trustee et les bénéficiaires, peuvent être obtenues ou sont accessibles en temps opportun par les autorités compétentes. Les pays devraient envisager de prendre des mesures pour faciliter l'accès aux informations sur les bénéficiaires effectifs et sur le contrôle des structures juridiques par les institutions financières et les entreprises et professions non financières désignées lorsqu'elles mettent en œuvre les obligations des recommandations 10 et 22.

F. POUVOIRS ET RESPONSABILITÉS DES AUTORITÉS COMPÉTENTES ET AUTRES MESURES INSTITUTIONNELLES

RÉGLEMENTATION ET CONTRÔLE

26. Réglementation et contrôle des institutions financières *

Les pays devraient s'assurer que les institutions financières sont soumises à une réglementation et font l'objet d'un contrôle adaptés et qu'elles mettent efficacement en œuvre les recommandations du GAFI. Les autorités compétentes et les autorités de contrôle du secteur financier devraient prendre les mesures législatives ou réglementaires nécessaires pour empêcher les criminels ou leurs complices de détenir ou de devenir les bénéficiaires effectifs d'une participation significative ou de contrôle d'une institution financière, ou d'y occuper un poste de direction. Les pays ne devraient pas autoriser l'établissement de banques fictives ni la poursuite de leurs activités.

Pour les institutions financières soumises aux Principes fondamentaux, les mesures réglementaires et de contrôle applicables à des fins prudentielles et qui sont également pertinentes en matière de blanchiment de capitaux et de financement du terrorisme devraient s'appliquer d'une manière similaire à des fins de LBC/FT. Ceci devrait comprendre la mise en œuvre d'une surveillance consolidée au niveau du groupe à des fins de LBC/FT.
Les autres institutions financières devraient être agréées ou enregistrées, faire l'objet d'une réglementation adaptée et être soumises à un contrôle ou à une surveillance à des fins de LBC/FT compte tenu du risque de blanchiment de capitaux ou de financement du terrorisme du secteur dans lequel elles opèrent. Au minimum, lorsque les institutions financières fournissent des services de transfert de fonds ou de valeurs ou des services de change, elles devraient être agréées ou enregistrées et soumises à des systèmes efficaces de surveillance assurant le respect de leurs obligations nationales en matière de LBC/FT.

27. Pouvoirs des autorités de contrôle
Les autorités de contrôle devraient être dotées de pouvoirs satisfaisants, y compris celui de procéder à des inspections, pour contrôler ou surveiller les institutions financières afin d'assurer qu'elles respectent leurs obligations en matière de LBC/FT. A cette fin, elles devraient être autorisées à exiger des institutions financières la production de toute information pertinente et à imposer des sanctions conformément à la recommandation 35 en cas de non-respect de leurs obligations de LBC/FT. Les autorités de contrôle devraient disposer des pouvoirs d'imposer une gamme de sanctions disciplinaires et financières, y compris du pouvoir, le cas échéant, de retirer, limiter ou suspendre l'agrément de l'institution financière.
28. Réglementation et contrôle des entreprises et professions non financières désignées *
Les entreprises et professions non financières désignées devraient être soumises aux mesures de réglementation et de contrôle suivantes :
Les casinos devraient être soumis à un régime complet de réglementation et de contrôle visant à garantir qu'ils appliquent efficacement les mesures de LBC/FT nécessaires. Au minimum :

- les casinos devraient être agréés ;
- les autorités compétentes devraient prendre les mesures législatives ou réglementaires nécessaires pour empêcher les criminels ou leurs complices de détenir ou de devenir les bénéficiaires effectifs d'une participation significative ou de contrôle d'un casino, d'y occuper un poste de direction ou d'en être l'exploitant ;
- les autorités compétentes devraient s'assurer que le respect par les casinos de leurs obligations en matière de LBC/FT fait l'objet d'un contrôle efficace.

Les pays devraient s'assurer que les autres catégories d'entreprises et de professions non financières désignées sont soumises à des dispositifs efficaces de surveillance assurant qu'elles respectent leurs obligations en matière de LBC/FT. Ces mesures devraient être prises en fonction des risques. Cette surveillance peut être effectuée par (a) une autorité de contrôle ou (b) par l'organisme d'autorégulation pertinent, à condition qu'un tel organisme puisse garantir que ses membres respectent leurs obligations en matière de LBC/FT.
L'autorité de contrôle ou l'organisme d'autorégulation devrait également (a) prendre les mesures nécessaires pour empêcher les criminels ou leurs complices d'accéder au statut de professionnel agréé ou de détenir une participation significative ou de contrôle, de devenir les bénéficiaires effectifs d'une telle participation, ou d'occuper des fonctions de direction, par exemple en soumettant ces personnes à un test d'aptitude et d'honorabilité (fit and proper test) ; et (b) disposer de sanctions efficaces, proportionnées et dissuasives conformes à la recommandation 35 en cas de non-respect des obligations de LBC/FT.

AUTORITÉS OPÉRATIONNELLES ET AUTORITÉS DE POURSUITE PÉNALE
29. Cellules de renseignements financiers *
Les pays devraient instituer une cellule de renseignements financiers (CRF) servant de centre national pour la réception et l'analyse (a) des déclarations d'opérations suspectes et (b) des autres informations concernant le blanchiment de capitaux, les infractions sous-jacentes associées et le financement du terrorisme, et pour la dissémination du résultat de cette analyse. La CRF devrait pouvoir obtenir des informations supplémentaires des entités déclarantes et devrait avoir accès en temps opportun aux informations financières, administratives et aux informations des autorités de poursuite pénale nécessaires pour exercer correctement ses fonctions.

30. Responsabilités des autorités de poursuite pénale et autorités chargées des enquêtes *
Les pays devraient s'assurer que les autorités de poursuite pénale désignées sont responsables des enquêtes sur le blanchiment de capitaux et le financement du terrorisme dans le cadre des politiques nationales de LBC/FT. Au minimum, dans tous les cas portant sur des infractions ayant généré des profits majeurs, ces autorités de poursuite pénale désignées devraient mettre en place une enquête financière de manière proactive en parallèle à la poursuite des infractions de blanchiment de capitaux, des infractions sous-jacentes associées et de financement du terrorisme. Cela devrait inclure les cas où l'infraction sous-jacente associée a lieu en dehors de leur juridiction. Les pays devraient s'assurer que les autorités compétentes ont la

responsabilité de procéder promptement à l'identification, au dépistage et au déclenchement des actions de gel et de saisie de biens qui sont ou qui peuvent être soumis à confiscation ou qui sont suspectés de constituer le produit du crime. Lorsque cela est nécessaire, les pays devraient également pouvoir recourir à des groupes multidisciplinaires permanents ou temporaires spécialisés dans les enquêtes financières ou sur les biens. Les pays devraient s'assurer, lorsque cela est nécessaire, que des enquêtes en coopération avec les autorités compétentes appropriées d'autres pays ont lieu.

31. Pouvoirs des autorités de poursuite pénale et des autorités chargées des enquêtes

Lors d'enquêtes sur le blanchiment de capitaux, les infractions sous-jacentes associées ou le financement du terrorisme, les autorités compétentes devraient pouvoir avoir accès à tous les documents et informations nécessaires pour les utiliser dans le cadre de ces enquêtes et des poursuites et actions qui s'y rapportent. Ceci devrait inclure les pouvoirs d'appliquer des mesures coercitives pour la production de documents détenus par les institutions financières, les entreprises et professions non financières désignées ou d'autres personnes physiques ou morales, pour la fouille de personnes et de locaux, pour recueillir des témoignages et pour la saisie et l'obtention de preuves.

Les pays devraient s'assurer que les autorités compétentes qui mènent des enquêtes peuvent utiliser une vaste gamme de techniques d'enquêtes spécifiques adaptées aux enquêtes sur le blanchiment de capitaux, les infractions sous-jacentes associées et le financement du terrorisme. Ces techniques d'enquêtes comprennent : les opérations sous couverture, l'interception de communications, l'accès aux systèmes informatiques et la livraison surveillée. En outre, les pays devraient disposer de mécanismes efficaces leur permettant de déterminer en temps opportun si des personnes physiques ou morales détiennent ou contrôlent des comptes. Ils devraient également assurer que les autorités compétentes disposent d'un mécanisme d'identification des biens sans notification préalable au propriétaire. Lors de la conduite d'enquêtes sur le blanchiment de capitaux, les infractions sous-jacentes associées et le financement du terrorisme, les autorités compétentes devraient pouvoir demander toutes les informations pertinentes détenues par la CRF.

32. Passeurs de fonds *

Les pays devraient avoir en place des mesures pour détecter les transports physiques transfrontaliers d'espèces et d'instruments négociables au porteur, y compris un système de déclaration et/ou de communication.

Les pays devraient s'assurer que leurs autorités compétentes ont le pouvoir de bloquer ou retenir les espèces ou instruments négociables au porteur suspectés d'être en rapport avec le financement du terrorisme, le blanchiment de capitaux ou des infractions sous-jacentes, ou faisant l'objet d'une fausse déclaration ou communication.

Les pays devraient s'assurer que des sanctions efficaces, proportionnées et dissuasives sont applicables aux personnes qui ont effectué une fausse déclaration ou une communication d'informations fausses. Lorsque des espèces ou instruments négociables au porteur sont liés au financement du terrorisme, au blanchiment de capitaux ou à des infractions sous-jacentes, les pays devraient aussi adopter des mesures, y compris de nature législative, conformes à la recommandation 4, autorisant la confiscation de ces espèces ou instruments.

OBLIGATIONS GÉNÉRALES

33. Statistiques

Les pays devraient tenir des statistiques complètes sur les questions relatives à l'effectivité et à l'efficacité de leur système de LBC/FT. Elles devraient comprendre des statistiques sur les DOS reçues et disséminées, les enquêtes sur le blanchiment de capitaux et le financement du terrorisme, les poursuites et condamnations liées au blanchiment de capitaux et au financement du terrorisme, les biens gelés, saisis ou confisqués et l'entraide judiciaire ou autres demandes internationales de coopération.

34. Lignes directrices et retour d'informations

Les autorités compétentes, les autorités de contrôle et les organismes d'autorégulation devraient établir des lignes directrices et assurer un retour d'informations qui aideront les institutions financières et les entreprises et professions non financières désignées dans l'application des mesures nationales de LBC/FT, et, en particulier, à détecter et déclarer les opérations suspectes.

SANCTIONS

35. Sanctions

Les pays devraient s'assurer qu'une gamme de sanctions efficaces, proportionnées et dissuasives, pénales, civiles ou administratives, est applicable aux personnes physiques et morales visées par les recommandations 6 et 8 à 23 qui ne respectent pas les obligations en matière de LBC/FT. Les sanctions devraient être applicables non seulement aux institutions financières et aux entreprises et professions non financières désignées, mais également à leurs dirigeants.

G. COOPÉRATION INTERNATIONALE

36. Instruments internationaux

Les pays devraient prendre des mesures immédiates pour devenir parties à la Convention de Vienne de 1988, la Convention de Palerme de 2000, la Convention des Nations Unies contre la corruption de 2003 et la Convention sur le financement du terrorisme de 1999 et pour les mettre pleinement en œuvre. Le cas échéant, les pays sont également encouragés à ratifier et à mettre en œuvre d'autres conventions internationales pertinentes telles que la Convention du Conseil de l'Europe sur la cybercriminalité de 2001, la Convention interaméricaine contre le terrorisme de 2002 et la Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme de 2005.

37. Entraide judiciaire

Les pays devraient, de manière rapide, constructive et efficace, fournir l'entraide judiciaire la plus large possible pour les enquêtes, les poursuites et les procédures connexes ayant trait au blanchiment de capitaux, aux infractions sous-jacentes associées et au financement du terrorisme. Les pays devraient disposer d'une base juridique adéquate pour fournir cette assistance et, le cas échéant, devraient disposer de traités, accords ou autres mécanismes permettant d'accroître la coopération. En particulier, les pays :

(a) ne devraient pas interdire ou assortir de conditions déraisonnables ou indûment
(b) restrictives l'octroi de l'entraide judiciaire ;
(c) devraient s'assurer qu'ils disposent de procédures claires et efficientes pour l'établissement des priorités et l'exécution en temps opportun des demandes d'entraide judiciaire. Les pays devraient avoir recours à une autorité centrale ou à un autre mécanisme officiel établi pour la transmission et l'exécution efficaces des demandes. Afin de suivre l'avancement des demandes, un système de gestion des dossiers devrait être en place ;
(d) ne devraient pas refuser d'exécuter une demande d'entraide judiciaire pour l'unique motif que l'infraction est également considérée comme portant sur des questions fiscales ;
(e) ne devraient pas refuser d'exécuter une demande d'entraide judiciaire au motif que leurs lois imposent la préservation du secret ou de la confidentialité aux institutions financières ou aux entreprises et professions non financières désignées (à l'exception des cas où l'information recherchée est détenue dans des circonstances relevant du secret professionnel légal ou d'un privilège professionnel légal) ;
(f) devraient préserver la confidentialité des demandes d'entraide judiciaire qu'ils reçoivent et des informations qu'elles contiennent, sous réserve des principes fondamentaux du droit interne, afin de protéger l'intégrité de la demande de renseignements ou de l'enquête. Si le pays requis ne peut pas respecter les obligations de confidentialité, il devrait en informer promptement le pays requérant.

Les pays devraient fournir l'entraide judiciaire malgré l'absence de double incrimination si l'assistance n'implique pas d'actions coercitives. Les pays devraient envisager d'adopter les mesures nécessaires leur permettant de fournir une large assistance en l'absence de double incrimination.

Lorsque la double incrimination est exigée pour l'entraide judiciaire, cette obligation devrait être considérée comme remplie, que les deux pays classent ou non l'infraction dans la même catégorie d'infractions, ou qu'ils utilisent ou non la même terminologie pour la désigner, lorsque les deux pays incriminent l'acte qui est à la base de l'infraction.

Les pays devraient s'assurer que parmi les pouvoirs et techniques d'enquête prévus par la recommandation 31 et parmi les autres pouvoirs et techniques d'enquête mis à la disposition de leurs autorités compétentes :

tous ceux liés à la production, à la perquisition et à la saisie d'informations, de documents ou d'éléments de preuve (y compris des pièces de nature financière) détenus par les institutions financières ou autres personnes, et au recueil de témoignages ; et une vaste gamme d'autres pouvoirs et techniques d'enquête peuvent également être utilisés en réponse à une demande d'entraide judiciaire et, lorsque cela est conforme à leur dispositif interne, en réponse à une demande directe adressée par des autorités judiciaires ou de poursuite pénale étrangères à leurs homologues nationaux.

Afin d'éviter les conflits de compétence, les pays devraient étudier la possibilité d'élaborer et de mettre en œuvre des mécanismes permettant de déterminer, dans l'intérêt de la justice, le lieu de saisine le plus approprié pour les poursuites de personnes mises en cause dans des cas sujets à des poursuites dans plusieurs pays.

Les pays devraient, lorsqu'ils formulent des demandes d'entraide judiciaire, faire tout leur possible pour fournir des informations factuelles et juridiques, indiquant notamment le degré d'urgence, afin de permettre une exécution efficiente et en temps opportun des demandes, et devraient envoyer les demandes par des moyens de transmission rapide. Les pays devraient, avant l'envoi des demandes, tout mettre en œuvre afin de s'assurer des exigences et formalités légales nécessaires à l'obtention de l'assistance.

Les autorités responsables de l'entraide judiciaire (par exemple, une autorité centrale) devraient bénéficier de ressources financières, humaines et techniques suffisantes. Les pays devraient mettre en place des procédures visant à s'assurer que le personnel de ces autorités respecte des normes professionnelles strictes, notamment en matière de confidentialité, fait preuve d'une grande intégrité et est doté de compétences appropriées.

38. Entraide judiciaire : gel et confiscation *

Les pays devraient s'assurer qu'ils disposent du pouvoir de prendre des actions expéditives en réponse aux demandes de pays étrangers d'identifier, de geler, de saisir et de confisquer les biens blanchis, les produits du blanchiment de capitaux, d'infractions sous-jacentes et du financement du terrorisme, les instruments utilisés ou destinés à être utilisés pour commettre ces infractions ou des biens d'une valeur correspondante. Ce pouvoir devrait comprendre celui de répondre aux demandes fondées sur des procédures de confiscation sans condamnation préalable et des mesures provisoires associées, à moins que cela ne contrevienne aux principes fondamentaux de leur droit interne. Les pays devraient également disposer de mécanismes efficaces pour gérer ces biens, instruments ou biens de valeur équivalente et s'appuyer sur des mesures visant à coordonner les procédures de saisie et de confiscation, parmi lesquelles le partage des avoirs confisqués.

39. Extradition

Les pays devraient sans retard indu exécuter de manière constructive et efficace les demandes d'extradition en matière de blanchiment de capitaux et de financement du terrorisme. Les pays devraient également prendre toutes les mesures possibles afin de s'assurer qu'ils ne fournissent pas un refuge aux personnes poursuivies pour des faits de financement du terrorisme, des actes terroristes ou des organisations terroristes. En particulier, les pays :

(a) devraient garantir que le blanchiment de capitaux et le financement du terrorisme constituent des infractions pouvant donner lieu à extradition ;
(b) devraient s'assurer qu'ils disposent de procédures claires et efficientes pour l'exécution en temps opportun des demandes d'extradition, y compris, le cas échéant, pour l'établissement de priorités. Afin de suivre l'avancement du traitement des demandes, un système de gestion des dossiers devrait être mis en place ;
(c) ne devraient pas assortir l'exécution des demandes de conditions déraisonnables ou indûment restrictives ;
(d) devraient s'assurer qu'ils disposent d'un cadre juridique adapté pour l'extradition.

Les pays devraient extrader leurs nationaux. Lorsqu'ils ne le font pas pour des raisons uniquement liées à la nationalité, les pays devraient, à la demande du pays requérant l'extradition, soumettre l'affaire sans retard indu à leurs autorités compétentes afin que des poursuites portant sur les infractions mentionnées dans la demande soient engagées. Ces autorités devraient prendre leurs décisions et conduire leurs procédures comme elles le feraient dans le cas de toute autre infraction grave selon leur droit interne. Les pays concernés devraient coopérer, en particulier pour les aspects concernant la procédure et la preuve, afin d'assurer l'efficacité de telles poursuites.

Lorsque la double incrimination est exigée pour l'extradition, cette obligation devrait être considérée comme remplie, que les deux pays classent ou non l'infraction dans la même catégorie d'infractions, ou qu'ils utilisent ou non la même terminologie pour la désigner, lorsque les deux pays incriminent l'acte qui est à la base de l'infraction.

Conformément aux principes fondamentaux du droit interne, les pays devraient disposer de mécanismes simplifiés d'extradition, par exemple en autorisant la transmission directe des demandes d'arrestation provisoire entre les autorités compétentes, l'extradition des personnes sur le seul fondement d'un mandat d'arrêt ou d'un jugement ou l'extradition simplifiée des personnes acceptant de renoncer à la procédure formelle d'extradition. Les autorités responsables de l'extradition devraient bénéficier de ressources financières, humaines et techniques suffisantes. Les pays devraient mettre en place des procédures visant à s'assurer que le personnel de ces autorités respecte des normes professionnelles strictes, notamment en matière de confidentialité, fait preuve d'une grande intégrité et est doté de compétences appropriées.

40. Autres formes de coopération internationale *

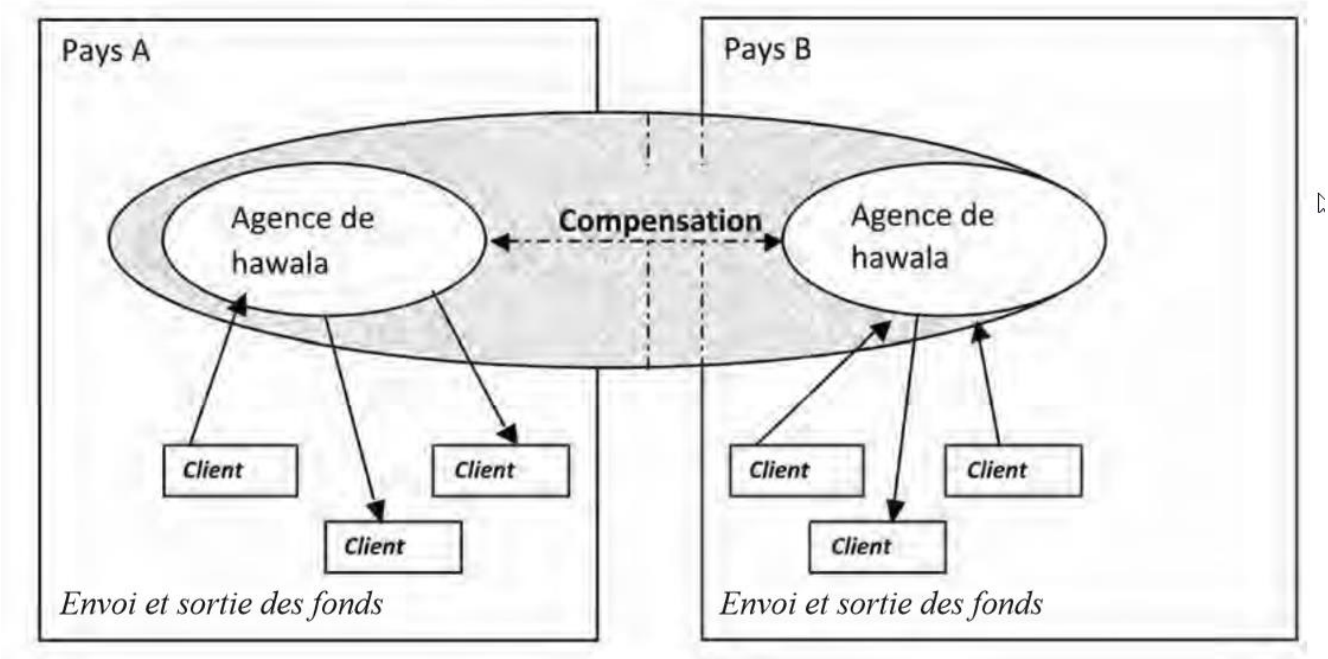
Les pays devraient s'assurer que leurs autorités compétentes peuvent, de manière rapide, constructive et efficace, accorder la coopération internationale la plus large possible en matière de blanchiment de capitaux, d'infractions sous-jacentes associées et de financement du terrorisme. Les pays devraient coopérer à la fois spontanément et sur demande et devraient fonder cette coopération sur une base légale. Les pays devraient autoriser leurs autorités compétentes à utiliser les moyens les plus efficaces pour coopérer. Si une autorité compétente a besoin d'accords ou d'arrangements bilatéraux ou multilatéraux tels que des protocoles d'accord, ceux-ci devraient être négociés et signés en temps opportun avec le plus grand nombre possible d'homologues étrangers.

Les autorités compétentes devraient utiliser des canaux ou mécanismes clairs pour la transmission et l'exécution efficaces des demandes d'informations ou d'autres types d'assistance. Les autorités compétentes devraient disposer de procédures

claires et efficientes pour l'établissement des priorités et l'exécution en temps opportun des demandes, ainsi que pour la protection des informations reçues.

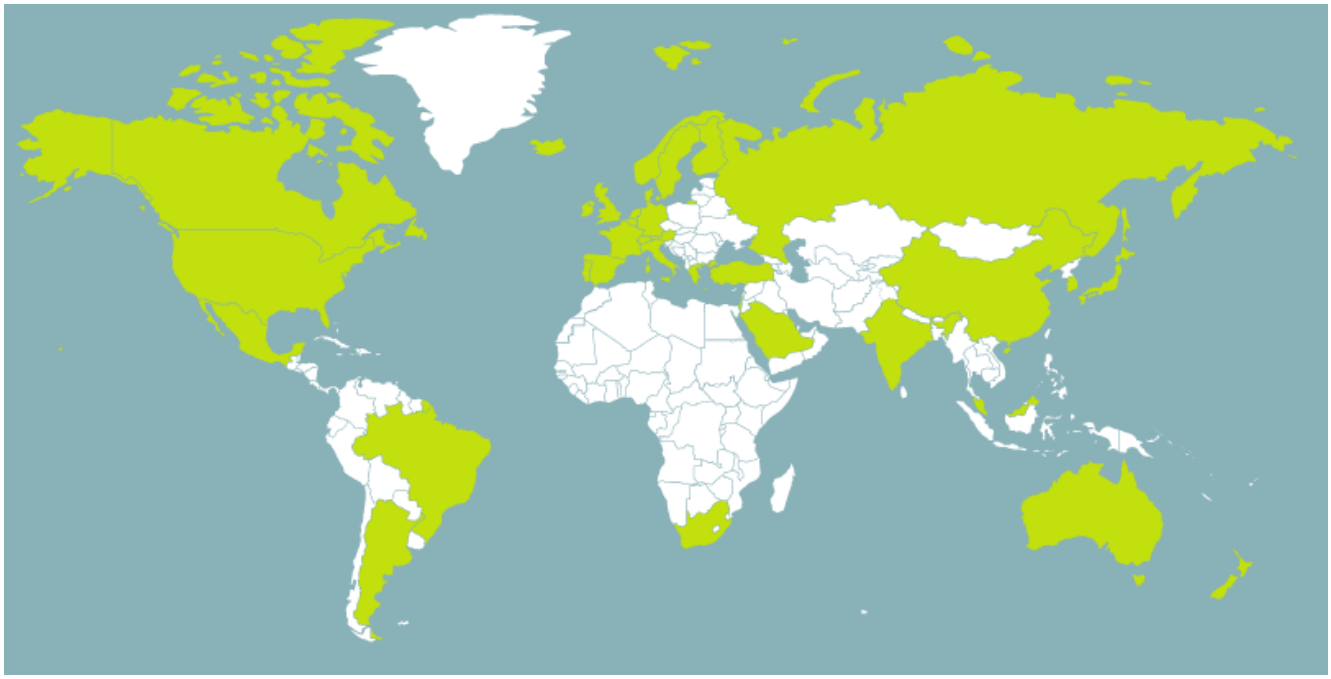
Source : FATF-GAFI, 2012, pp.10-29

Annexe 2 : Le fonctionnement de l'*hawala*



Source : MAHAMOUD, 2014, p.51

Annexe 3 : Les membres du GAFI



Afrique du Sud, Allemagne, Arabie Saoudite Argentine, Australie, Autriche, Belgique, Brésil, Canada, Chine, Commission Européenne, Conseil de coopération du golfe , Corée (République démocratique), Danemark Espagne, Etats-Unis, Fédération de Russie, Finlande, France, Grèce, Hong Kong (Chine) Inde, Irlande, Islande, Israël, Italie, Japon, Luxembourg, Malaisie, Mexique, Norvège, Nouvelle-Zélande, Pays-Bas (Royaume des), Portugal, Royaume-Uni, Singapour, Suède, Suisse, Turquie

Source : FATF-GAFI, 2019b

Annexe 4 : Le formulaire de déclaration de soupçon

Modèle de déclaration concernant un soupçon de BC/FTP en application de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces

---

1. DECLARANT (article 5, § 1 de la Loi)
(Identification et coordonnées de contact)

---

2. CLIENT (article 21 de la Loi)
A mentionner : toutes les données d'identification requises en vertu de l'article 26 de la Loi

---

3. MANDATAIRE(S) DU CLIENT (article 22 de la Loi)
A mentionner : toutes les données d'identification requises en vertu de l'article 26 de la Loi

---

4. BENEFICIAIRES EFFECTIFS (article 23 de la Loi) :
À savoir la ou les personnes physiques qui, en dernier ressort, possèdent ou contrôlent le client, le mandataire du client ou le bénéficiaire des contrats d'assurance-vie (comme défini à l'article 4, 27°, deuxième paragraphe de la Loi), et/ou la ou les personnes physiques pour lesquelles une opération est exécutée ou une relation d'affaires nouée (comme défini à l'article 4, 27°, troisième paragraphe de la Loi)

A mentionner : toutes les données d'identification requises en vertu de l'article 26 de la Loi

---

5. BENEFICIAIRES DES CONTRATS D'ASSURANCES-VIE (article 24 de la Loi)
A mentionner : toutes les données d'identification requises en vertu de l'article 26 de la Loi

---

6. AUTRES PERSONNES INTERVENANT DANS L'OPERATION OU DANS LES FAITS

A mentionner : les données d'identification (voir points précédents) d'autres personnes physiques ou morales ou de constructions juridiques intervenant dans l'opération comme donneur d'ordre, garant, contrepartie ou banque intermédiaire ou autre intermédiaire, ou qui jouent un rôle dans les faits déclarés

_____

7. DESCRIPTION DES CARACTERISTIQUES DU CLIENT ET DE L'OBJET ET DE LA NATURE DE LA RELATION D'AFFAIRES OU DE L'OPERATION OCCASIONNELLE (article 34 de la Loi)

_____

8. DESCRIPTION DES FONDS, DES OPERATIONS OU TENTATIVES D'OPERATIONS OU DES FAITS

Nature des fonds, des opérations ou tentatives d'opérations ou des faits qui peuvent constituer un indice de blanchiment ou de financement du terrorisme ou de la prolifération, montant, devise, lieu (nom et adresse de l'agence), date, etc.

_____

9. EXECUTION DE L'OPERATION

Délai dans lequel l'opération va être exécutée par le déclarant. Si l'opération est exécutée avant que la CTIF ne soit informée, donner les raisons pour lesquelles la CTIF n'a pas été informée préalablement.

_____

10. INDICES DE BLANCHIMENT DE CAPITAUX OU DE FINANCEMENT DU TERRORISME/PROLIFERATION

Indices laissant présumer que les faits sont liés au BC/FTP ou à une tentative de BC/FTP

_____

11. ENQUETE PENALE

Signaler ici si une enquête pénale est déjà en cours ou s'il y a des contacts entre le déclarant et une autorité judiciaire ou un service de police. Le cas échéant, mentionner la référence du dossier ou l'identité de la personne de contact.

---

12. COMMENTAIRES EVENTUELS

---

13. ANNEXES

Date
Nom et fonction du signataire
Signature

Notez qu'aujourd'hui, la plupart des déclarations de soupçon s'effectuent via un système en ligne permettant aux déclarants de remplir et d'envoyer directement leurs déclarations par internet. Toutefois, cette annexe donne un aperçu des informations demandées par la Cellule.

Source : CTIF, 2019

Annexe 5 : Le plan de l'interview

Introduction

Avant de commencer, je tiens à vous remercier pour votre disponibilité et votre participation à cette étude. Je mène cette recherche dans le cadre de la réalisation de mon mémoire qui analyse l'approche fondée sur les risques dans la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Je vais vous poser une série de questions, vous êtes totalement libre dans la manière d'y répondre car il n'y a pas de bonne ou de mauvaise réponse, soyez simplement spontané et clair.

Dans le cadre de l'accord de confidentialité signé avec votre société, toutes les informations qui seront susceptibles de vous identifier vous ou l'entreprise ne seront pas publiées et votre témoignage restera bien-sûr anonyme. J'aimerais enregistrer cette conversation, y voyez-vous un inconvénient?

Echauffement

Permettez-moi de me présenter. Je m'appelle Aurélie, j'ai 23 ans et je suis en 2ème année de master en ingénieur de gestion à l'Université de Namur. Je rédige actuellement mon mémoire sur l'évaluation globale des risques dans la lutte contre le blanchiment de capitaux et le financement du terrorisme afin d'obtenir mon diplôme d'ingénieur de gestion.

A présent, je vais vous demander de vous présenter en quelques mots comme je viens de le faire.

Quelle est votre fonction au sein de cet établissement de crédit ? En quoi cela consiste-t-il ?

Topo général : la Loi du 18 septembre 2017

Pouvez-vous m'en dire plus à propos de l'impact concret que cette mise à jour législative a eu sur la société ? (politique interne, procédures, formations, investissements …)

Quels sont les différents coûts engendrés par la mise en place de l'approche par les risques au sein de la banque ?

Les sources d'informations sont multiples pour les entités assujetties. Sur quoi vous basez vous principalement pour mettre en place l'ensemble des obligations requises par l'approche par les risques ? (BNB et circulaire ? Directive de l'Europe ? Feedback de la CTIF ? Outils externes ?)

Comment gérez-vous les mises à jour récurrentes de cette règlementation en matière de LBC/FT ?

Discussion spécifique : l'évaluation globale des risques et les enjeux

Pourriez-vous m'expliquer ce qu'est l'évaluation globale des risques et quel est l'intérêt de celle-ci ?

Quel est votre rôle en regard de cette évaluation ?

Parlez-moi de sa mise en place au sein de la société. Comment avez-vous intégré cette évaluation au sein de cette grande entreprise belge ?

Quels sont les outils concrets fournis par les autorités pour vous aider dans la réalisation de cette évaluation ? Lesquels utilisez-vous le plus ?

Avez-vous déjà été face à des interrogations auxquelles la législation ne fournissait aucune réponse ? Lesquelles ? Quelles solutions avez-vous finalement mises en place ?

Au vu des évaluations globales déjà réalisées ces dernières années, diriez-vous que ce processus d'évaluation des risques est plutôt objectif ou subjectif ? Pourquoi ?

Selon la Loi, cette évaluation doit se faire périodiquement et s'actualiser. Quel est l'intérêt de cette obligation ?

Comment vous positionnez-vous par rapport aux obligations de détection de fraude, de blanchiment ou de financement du terrorisme qui incombent maintenant à votre société ?

Quels sont pour vous les principaux enjeux de l'évaluation globale des risques pour les prochaines mois ou années à venir ?

En conclusion, comment évalueriez-vous l'efficience des mesures actuelles et songez-vous à certaines modifications ou recommandations ?

A titre personnel, pensez-vous que tout le système de lutte contre le BC/FT mis en place en Belgique a un réel impact sur ces deux infractions ?

Conclusion

Avez-vous quelque chose à rajouter? Un point, une critique ou une conclusion que je n'aurai pas eu l'occasion d'aborder ?

Annexe 6 : L'évaluation globale des risques dans la Loi AML

Article 16

Les entités assujetties prennent des mesures appropriées et proportionnées à leur nature et à leur taille pour identifier et évaluer les risques de BC/FT auxquels elles sont exposées, en tenant compte, notamment, des caractéristiques de leurs clientèles, des produits, services ou opérations qu'elles proposent, des pays ou zones géographiques concernées, et des canaux de distribution auxquels elles ont recours.

Elles prennent au moins en considération, dans leur évaluation globale des risques visée à l'alinéa 1er, les variables énoncées à l'annexe I. Par ailleurs, elles peuvent tenir compte des facteurs indicatifs d'un risque potentiellement moins élevé énoncés à l'annexe II, et tiennent compte au minimum des facteurs indicatifs d'un risque potentiellement plus élevé énoncés à l'annexe III.

Elles tiennent également compte des conclusions pertinentes du rapport établi par la Commission européenne en vertu de l'article 6 de la Directive 2015/849, du rapport établi par les organes de coordination en application de l'article 68, chacun pour ce qui les concerne, ainsi que de toute autre information pertinente dont elles disposent.

Article 17

L'évaluation globale des risques visée à l'article 16 est documentée, mise à jour et tenue à la disposition des autorités de contrôle compétentes en vertu de l'article 85.

Les entités assujetties doivent être en mesure de démontrer à leur autorité de contrôle compétente en vertu de l'article 85 que les politiques, les procédures et les mesures de contrôle interne qu'elles définissent conformément à l'article 8, y compris, le cas échéant, les politiques d'acceptation des clients, sont appropriées au regard des risques de BC/FT qu'elles ont identifiés.

La mise à jour de l'évaluation globale des risques implique, le cas échéant, que soient également mises à jour les évaluations individuelles des risques visées à l'article 19, § 2, alinéa 1er.

Article 18

Les autorités de contrôle compétentes en vertu de l'article 85 peuvent décider que certaines évaluations des risques documentées ne sont pas nécessaires si les risques propres aux activités concernées sont bien précisés et compris.

Source : Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces

Annexe 7 : Un exemple de support de BWRA

Catégorie de risque - Sous-catégorie *(max. 200 caractères par cellule)*		**Exposition** *(max. 200 caractères par cellule)*	**Mesures existantes de gestion des risques** *(max. 200 caractères par cellule)*
Cliënts	PPE	Elevée / Très élevée	Toutes les mesures art. 41 loi
	Entreprises publiques	(...)	(...)
Produits			
Services / Transactions			
(...)			

Adéquation de la gestion des risques *(max. 200 caractères par cellule)*	**Mesures nouvelles / complémentaires éventuelles** *(max. 200 caractères par cellule)*	**Timing et moyens** *(max 200 caractères par cellule)*
Non OK - Nombre très élevé de PPE provenant des pays à risque A et B	Acceptation des clients: la décision d'acceptation des PPE des pays A et B doit recevoir l'approbation complémentaire du Comité de direction	1 mois - Adaptation des procédures internes
(...)	(...)	(...)

Source : BNB, 2019

Annexe 8 : Le questionnaire du BWRA

1. Décrivez brièvement la méthodologie que vous utilisez pour l'évaluation globale des risques visée à l'article 16 de la loi BC/FT.

2. Avez-vous utilisé – en plus des critères légaux visés à l'article 16 de la loi BC/FT – d'autres critères et variables de risque complémentaires pour procéder à l'évaluation des risques? Expliquez votre réponse.

3. Si vous faites partie d'un groupe, si vous opérez via des filiales, succursales ou autres implantations (étrangères), ou si vous opérez par l'intermédiaire d'un point de contact central, veuillez exposer brièvement comment - à la lumière des articles 3 et 6 du Règlement BC/FT – vous avez intégré cette dimension dans la politique de risque du groupe.

4. Avez-vous l'intention - après évaluation de ce premier exercice - de prendre des mesures pour améliorer ou ajuster le processus d'analyse des risques ? Veuillez expliquer votre réponse.

5. Avez-vous dû, ou allez-vous devoir – à la suite de cet exercice – apporter des changements fondamentaux à votre gestion des risques BC/FT (par exemple en prenant de lourdes mesures de gestion des risques complémentaires, en renforçant les effectifs consacrés à la prévention BC/FT, en procédant à de grandes opérations de rattrapage pour remédier à des lacunes, etc.), ou avez-vous décidé de restreindre fortement ou de mettre fin à certaines activités (par exemple parce qu'il s'est avéré que le risque BC/FT était très difficile, voire impossible, à maîtriser) ? Veuillez expliquer votre réponse.

Source : BNB, 2019